Межсетевой экран Numa Edge

Установка и настройка утилиты numa-ssh

Листов 7

Санкт-Петербург
2022

ИДЕНТИФИКАЦИЯ ДОКУМЕНТА

Название документа	Установка и настройка утилиты numa-ssh
Версия документа	1.2
Идентификация ОО	Межсетевой экран Numa Edge
Идентификация разработчика	ООО «НумаТех»
Ключевые слова	Межсетевой экран, МЭ, numa-ssh

ВВЕДЕНИЕ

По умолчанию для протокола удаленного управления SSH в Numa Edge используется шифрование на основе стандартов ГОСТ 34.12-2018, ГОСТ 34.13-2018, а также аутентификация на основе стандарта ГОСТ 34.10-2012. По этой причине на клиентском устройстве требуется специальное ПО, которое позволит подключаться к Numa Edge, используя отечественные криптографические алгоритмы. Список данных пакетов представлен в таблице 1.

Таблица 1 — Deb пакеты из комплекта поставки

Название	**Описание**
libengine-gost-openssl<version>.deb	OpenSSL engine с поддержкой алгоритмов ГОСТ.
numa-openssh-client<version>.deb	OpenSSH клиент с добавленной поддержкой алгоритмов ГОСТ.

1. ПОДДЕРЖИВАЕМЫЕ ОС

1.1. Linux

В настоящий момент утилита numa-ssh распространяется исключительно в формате deb пакета и поэтому список поддерживаемых ОС ограничен семейством Debian-based дистрибутивов. Была протестирована корректность работы утилиты в следующих ОС:

Дистрибутив	**Каталог в архиве numa-ssh**
Debian 9 «Stretch»	debian9
Debian 10 «Buster»	debian10
Debian 11 «Bullseye»	debian11
Debian 12 «Bookworm»	debian12
Ubuntu 20.04 «Focal Fossa» (LTS)	debian10
Ubuntu 22.04 «Jammy Jellyfish» (LTS)	ubuntu22.04
Astra Linux Орел 2.12.40	debian9
Astra Linux Smolensk SE 1.6	debian9

1.2. Windows

На ОС семейства Windows утилита работает через подсистему *Windows Subsystem for Linux*. Для установки WSL воспользуйтесь следующей инструкцией: https://docs.microsoft.com/ru-ru/windows/wsl/install. При установке WSL 2.0 по умолчанию происходит установка последней LTS версии дистрибутива Ubuntu.

ПРИМЕЧАНИЕ: Обратите внимание, сама подсистема WSL, как и специальная сборка дистрибутива для WSL скачиваются с сайта компании Microsoft. По этой причине для установки WSL требуется доступ в интернет. Также в сети существуют инструкции по отдельному скачиванию образов дистрибутивов и подсистемы WSL с последующей установкой на устройствах, не имеющих доступ в интернет.

После завершения установки запустите установленную систему в консоли PowerShell с помощью команды:

```
PS C:\WINDOWS\system32> wsl
```

После выполнения команды, PowerShell переключится в Linux окружение. В этом можно убедиться, проверив переменную окружения *$SHELL*.

```
root@Windows10:/mnt/c/Users/admin# echo $SHELL
/bin/bash
root@Windows10:/mnt/c/Users/admin#
```

Дальнейшие действия по установке и настройке пакетов будут соответствовать действиям в поддерживаемых Linux дистрибутивах.

2. СОВМЕСТИМОСТЬ С ДРУГИМИ GOST ENGINE

Совместимость с другими OpenSSL Engine, добавляющим поддержку ГОСТ алгоритмов и утилиты numa-ssh, отсутствует. Если на используемой системе уже установлен какой-либо GOST Engine (gost-astra, rtengine и т.д.), его необходимо отключить в конфигурационном файле openssl.cnf.

3. УСТАНОВКА И НАСТРОЙКА ПАКЕТОВ

Установка выполняется от пользователя root или с использованием sudo.

Перед установкой рекомендуем обновить репозитории с помощью команды:

```
# apt-get update
```

Установите скачанные пакеты из каталога загрузки (при необходимости будут установлены зависимости):

```
# apt-get install ./libengine-gost-openssl1.1_1.1.0+p5_amd64.deb ./numa-openssh-client_8.4p1-5+numa1_amd64.deb
```

После установки создайте копию существующего конфигурационного файла openssl:

```
# cp /etc/ssl/openssl.{cnf,bcp}
```

Откройте конфигурационный файл /etc/ssl/openssl.cnf с помощью любого текстового редактора и добавьте в него следующие строки:

В начало файла, например, после первого комментария добавьте строку:

```
openssl_conf = openssl_def
```

ПРИМЕЧАНИЕ Обратите внимание, что в некоторых дистрибутивах конфигурационный файл openssl.cnf может уже содержать параметр openssl_conf, в котором уже указано значение секции по умолчанию.

Например, в дистрибутиве Debian 10 «Buster» содержится следующий параметр:

```
openssl_conf = default_conf
```

В таком случае, в зависимости от содержимого вашего конфигурационного файла:

закомментируйте данный параметр, если секция [default_conf] в конфигурации не встречается (настройки по умолчанию) и добавьте все секции из примера ниже.

добавьте в секцию [default_conf] параметр с описанием секции engine

```
engines = engine_section
```

Затем добавьте только секции [engine_section] и [gost_section] как из примера ниже.

В самый конец файла добавьте следующие строки

```
[openssl_def]
engines = engine_section

[engine_section]
gost = gost_section

[gost_section]
engine_id = gost
default_algorithms = ALL
CRYPT_PARAMS = id-Gost28147-89-CryptoPro-A-ParamSet
```

Для проверки корректности установки выполните команду для просмотра установленных engine для утилиты openssl. Должна быть выведена следующая конфигурация:

```
# openssl engine
(rdrand) Intel RDRAND engine
(dynamic) Dynamic engine loading support
(gost) Reference implementation of GOST engine
```

Для того чтобы убедиться, что ГОСТ алгоритмы поддерживаются утилитой numa-ssh, просмотрите доступные алгоритмы ключевого обмена, отфильтрованные по строке gost.

```
# numa-ssh -Q kex | grep gost
ecdh-gost2001-cpa
ecdh-gost2001-cpb
ecdh-gost2012-256-cpa
ecdh-gost2012-256-cpb
```

4. ПОДКЛЮЧЕНИЕ К NUMA EDGE

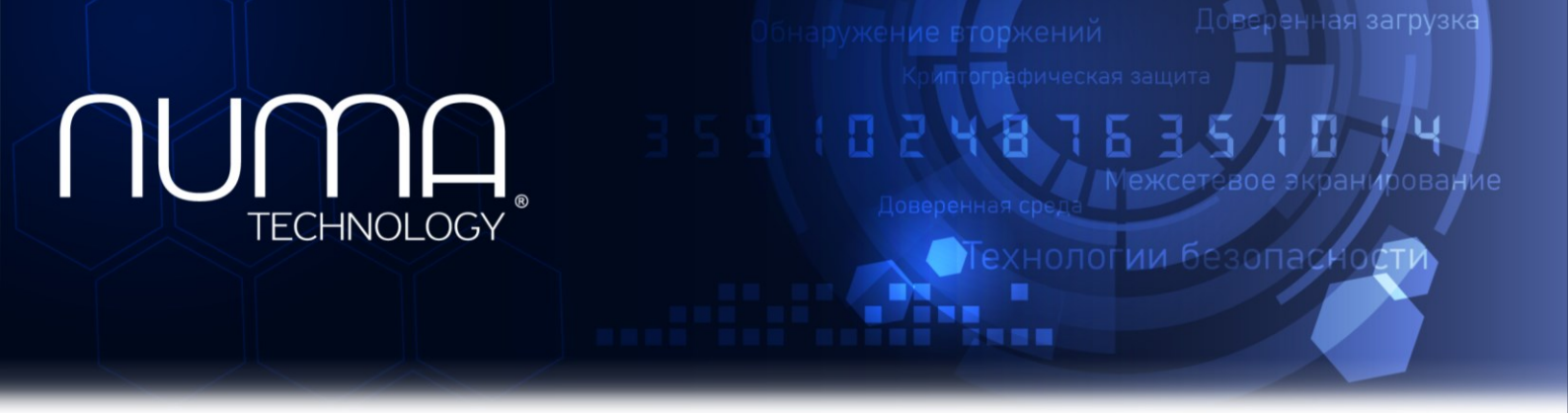
В случае успешной конфигурации, вы можете подключиться к Numa Edge через управляющий интерфейс с помощью команд:

```
# numa-ssh <username>@<ip-address>
```

При этом на клиенте должно быть настроено получение IP адреса по DHCP для интерфейса, подключенного к управляющему интерфейсу.

На ОС Windows, используя WSL, можно вызывать Linux команды из PowerShell, добавляя вначале команды *wsl*:

```
PS C:\WINDOWS\system32> wsl numa-ssh admin@192.168.200.1
The authenticity of host '192.168.200.1 (192.168.200.1)' can't be established.
ECDSA key fingerprint is SHA256:e+9ORU63tnNow+66/fg7CEpRb8nBfBmXYE8Ex9z7WgM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.200.1' (ECDSA) to the list of known hosts.
Edge 1.0
Password:
admin@edge:~$
```



Межсетевой экран Numa Edge

Руководство администратора

Листов 1561

Санкт-Петербург
2023

Содержание

1 Общие положения

1.1 Идентификация документа

Название документа	Руководство администратора
Версия документа	1.0.17
Обозначение документа	643.АМБН.00004-01 32 01
Идентификация ОО	Межсетевой экран Numa Edge
Идентификация разработчика	ООО «НумаТех»
Ключевые слова	Межсетевой экран, МЭ

1.2 Аннотация документа

Документ предназначен для ознакомления пользователя с технической информацией о межсететвом экране Numa Edge (далее – изделие) и содержит сведения о командах для управления межсетевым экраном.

2 Общие сведения

Изделие предназначено для выполнения следующих функций:

- контроль и фильтрация сетевого трафика;
- идентификация и аутентификация;
- регистрация событий безопасности (аудит);
- обеспечение бесперебойного функционирования и восстановления;
- тестирование и контроль целостности;
- преобразование сетевых адресов;
- маскирование;
- приоритизация информационных потоков;
- управление (администрирование);
- взаимодействие с другими средствами защиты информации;

Функции контроля и фильтрации сетевого трафика реализуются в соответствии с заданными правилами и политиками проходящих через него информационных потоков.

Механизм идентификации и аутентификации позволяет идентифицировать администраторов изделия. Аутентификационные данные администратора (логин и пароль) могут быть изменены в ходе эксплуатации изделия. Права администратора требуются для изменения настроек изделия, управления пользователями и изделием.

В ходе работы выполняется регистрация событий безопасности, установленных администратором. Журнал регистрации событий формируется из сообщений, поступающих при срабатывании механизмов защиты. Журнал регистрации событий возможно выгрузить на отдельный носитель информации.

Изделие при инсталляции автоматически создает резервные копии всех программных модулей. При сбое (несовпадении контрольных сумм файлов конфигурации, несовпадении контрольных сумм исполняемых фалов) администратор в ручном режиме осуществляется восстановление изделия в заводское состояние штатными средствами.

В ходе работы изделие производит самотестирование и контроль целостности ключевых блоков информации.

3 Структура документа

В этом руководстве даны указания по использованию основных функций изделия Межсетевой экран Numa Edge. Описаны имеющиеся команды и приведены примеры настройки.

В предисловии приведены сведения об использовании данного руководства. Рассматриваются следующие вопросы:

- кому предназначен документ;
- структура руководства;
- условные обозначения;

3.1 Кому предназначен документ

Данное руководство предназначено для опытных системных и сетевых администраторов. В зависимости от используемой функциональности, от читателей требуются знания в следующих областях:

- сети и связь с передачей данных;
- протоколы TCP/IP;
- общая настройка маршрутизаторов;
- протоколы маршрутизации;
- администрирование сетей;
- безопасность сетей.

3.2 Условные обозначения

В руководстве используются информационные абзацы, маркеры и соглашения о стиле текста.

3.3 Информационные абзацы

В руководстве используются следующие типы информационных абзацев:

Предупреждения извещают о ситуациях, которые могут нести угрозу личной безопасности, например:

ПРЕДУПРЕЖДЕНИЕ *Выключите питание с помощью главного рубильника перед тем, как попытаться подключить внешний кабель к дополнительному источнику питания в технологической коробке.*

Предостережения извещают о ситуациях, которые могут нанести вред системе или оборудованию либо привести к необходимости ремонта, например:

ПРЕДОСТЕРЕЖЕНИЕ *Перезапуск работающей системы приведет к перерыву в обслуживании.*

Примечания предоставляют сведения, которые могут потребоваться для предотвращения проблем или ошибок в настройке:

ПРИМЕЧАНИЕ *Перед тем, как включить сетевые интерфейсы для протоколов маршрутизации, необходимо создать их.*

4 Организационно-распорядительные меры

4.1 Процедуры поставки

4.1.1 Общий порядок поставки

При поставке изделия заказчику от среды производства до среды установки изготовитель выполняет следующие действия:

- расчет контрольных сумм файлов изделия;
- упаковка комплекта поставки;
- передача упакованного комплекта поставки на склад готовой продукции;
- выдача и/или отправка упакованного комплекта поставки заказчику.

4.1.2 Комплектность упаковки изделия

Упаковка изделия в общем случае содержит следующие комплектующие:

- компакт-диск с дистрибутивом изделия и дополнительной документацией;
- формуляр на изделие;
- руководство администратора.

4.1.3 Процедуры и меры безопасности при распространении изделия к месту назначения

Процедуры и меры безопасности при распространении изделия к месту назначения решают следующие задачи:

- обеспечивают идентификацию и целостность изделия во время пересылки изделия;
- обеспечивают обнаружение несанкционированных модификаций изделия;
- препятствуют попыткам подмены изделия от имени изготовителя.

Контроль целостности программного обеспечения, установленного на аппаратную платформу

Расчет эталонных контрольных сумм (далее – КС) файлов изделия, установленного на аппаратную платформу, осуществляется на этапе сборки изделия. При включении изделие выполняет контроль целостности установленных файлов до запуска программы. При выявлении несоответствия сохраненным значениям на монитор выводится уведомление об этом событии. Расчет КС должен производится согласно документу «Инструкция по проверке КС», находящейся в комплекте поставки.

Контроль целостности файлов установочного компакт-диска

Контроль целостности файлов, находящихся на компакт диске проверяются путем расчета и сравнение КС изделия с эталонными КС, записанными в документе «Формуляр». Расчет КС должен производится согласно документу «Инструкция по проверке КС», находящейся в комплекте поставки.

Контроль сохранности упакованного комплекса

Готовое изделие с документацией на него помещают в полиэтиленовый пакет. Пакет помещают в картонную коробку, которую заклеивают скотчем с символикой изготовителя (ООО «НумаТех»). Упакованное изделие до отправки заказчику хранится на складе готовой продукции.

4.2 Требование безопасности к среде ИТ

Изделие обеспечивает функциональное назначение при реализации пользователем следующих предварительных организационно-распорядительных мер:

- установка (переустановка, обновления) изделия должны осуществляться с оригинальных лицензионных дистрибутивных носителей (копий эталонных компакт-дисков) или инсталляционного (-ных) файла(-ов) (или архивов их содержащих), размещённых в специальном разделе сайта изготовителя, и полученных установленным порядком;

- изменение версии ПО изделия на другую версию возможно только в том случае, если изготовителем подтверждено соответствие данной версии ПО изделия требованиям безопасности информации путем проведения анализа уязвимостей и периодических испытаний изделия и его ПО;
- необходимо наличие администратора безопасности, отвечающего за правильную эксплуатацию и настройку изделия;
- необходимо сохранение в секрете идентификаторов (имен) и паролей (кодов) администратора изделия;

К среде ИТ, в которой функционирует изделие, предъявляются следующие требования безопасности, относящиеся к пользователю:

- обеспечение регламента доступа непривилегированных пользователей из внешней сети в защищаемые сети по всем типам протоколов, за исключением специально созданной для такого доступа демилитаризованной сети;
- обеспечение физической сохранности технических средств (межсетевого экрана, СВТ, на котором он функционирует и терминалов, с которых выполняется его управление) и исключение возможности доступа к ним посторонних лиц;
- обеспечение установки, конфигурирования и управления изделия в соответствии с эксплуатационной документацией.

4.3 Требования по безопасной приемке Изделия

При получении Изделия заказчик должен:

- обследовать поставку на предмет полноты комплектности. Комплект поставки должен состоять из частей, описанных в п. 4.1.2. Состав дополнительной документации на компакт-диске должен соответствовать таблице 6 документа Формуляр;
- убедиться, что в документах Формуляр и Паспорт заполнены все необходимые графы, стоят соответствующие печати и подписи, Формуляр Изделия промаркирован идентификатором СЗИ;
- убедиться, что компакт-диск расположен в конверте, заклеенном наклейкой с логотипом ООО «НумаТех», отсутствуют видимые признаки вскрытия конверта, а прописанный идентификатор СЗИ и номер экземпляра совпадают с теми, что прописаны в Формуляре на Изделие;
- убедиться, что комплектация полученного аппаратного исполнения Изделия соответствует сведениям, приведенным в таблице 6 документа Паспорт;
- проверить физическую целостность аппаратного исполнения Изделия на предмет отсутствия механических повреждений и наличия маркировочных этикеток на поверхности корпуса Изделия и упаковочной тары;
- ознакомиться с документацией на Изделие;
- перед эксплуатацией Изделия необходимо провести контроль целостности неизменных файлов Изделия согласно документу «Инструкция по проверке контрольных сумм» 643.АМБН.00004-01 88 01, входящему в комплект поставки.

ПРИМЕЧАНИЕ. Убедиться, что в документе «Сервисный сертификат», входящего в комплект поставки, имеются отметка о дате продажи, печать продавца и сведения об уполномоченном представителе продавца. Без данных отметок техническая поддержка и гарантийное обслуживание Изделия будут недоступны.

4.4 Настройка программы

Для настройки изделия необходимо выполнить установку изделия:

- установить изделие на СВТ в серверный шкаф или на рабочее место (в зависимости от форм-фактора изделия) и закрепить его;
- осуществить подключение изделия к ПЭВМ, с которого будет осуществляться его управление и настройка;
- подключение производится путем установки штатного Ethernet-кабеля в управляющий порт изделия и в соответствующий разъем ПЭВМ.

Выбранный для связи с управляющим портом интерфейс Ethernet должен быть настроен на ЭВМ на автоматическое получение IP-адреса по протоколу DHCP.

Настройка изделия проводится после окончания монтажа изделия на объекте и в процессе эксплуатации.

Настройка включает в себя:

- установку пользовательского интерфейса на ПЭВМ (только при первом включении);
- настройка конфигурационной части изделия.

5 Использование интерфейса командной строки

В данном разделе представлен обзор интерфейса командной строки Numa Edge, являющегося основным интерфейсом пользователя для системы Numa Edge.

В данном разделе рассматриваются следующие вопросы:

- Возможности интерфейса командной строки
- Основные команды интерфейса командной строки

5.1 Возможности интерфейса командной строки

В данном разделе рассматриваются следующие вопросы:

- Доступ к интерфейсу командной строки
- Интерфейс командной строки и интерпретатор команд системы Numa Edge
- Уровни полномочий пользователя
- Режимы интерфейса
- Запросы для ввода команд
- Использование специальных символов в командах
- Автодополнение команд
- Журнал команд
- Правка команд
- Фильтрация вывода команд
- Отображение длинного вывода
- Работа с конфигурацией
- Выполнение эксплуатационной команды из режима настройки
- Отображение конфигурации из эксплуатационного режима

5.1.1 Доступ к интерфейсу командной строки

Доступ к интерфейсу командной строки Numa Edge можно получить при подключение к устройству:

- через последовательный порт;
- удаленно при помощи сеанса SSH.

При подключении через последовательный порт (RS-232) используются следующие параметры:

- скорость: 115200 бит/с;
- без контроля четности (No parity);
- 8 бит данных (8 data bits);
- 1 стоповый бит (1 stop bits).

При использовании подключения через последовательный порт могут возникнуть проблемы при отображении кириллических символов.

После завершения процесса загрузки Numa Edge появится запрос на вход в систему:

- при подключении через последовательный порт

```
Numa Edge 1.0
edge login:
```

- при подключении через SSH

```
login as:
```

Для входа в систему используется идентификатор пользователя и пароль определенной учетной записи пользователя. По умолчанию в системе присутствует единственная предварительно определенная учетная запись пользователя с реквизитами, приведенными в таблице ниже.

Таблица 1 – Реквизиты учетной записи пользователя по умолчанию в Numa Edge

Параметр	**Значение**
Идентификатор пользователя:	admin
Пароль по умолчанию:	admin

По умолчанию системой назначается пароль '`admin`', но в случае его замены новый пароль должен соответствовать требованиям к устанавливаемому паролю и содержать не менее 10 символов.

Данный пользователь обладает полномочиями уровня администратора, что позволяет выполнять все команды Numa Edge и операционной системы. При автодополнении команд и в справке по интерфейсу командной строки отображаются только команды Numa Edge.

С помощью команд операционной системы можно изменить учетные записи пользователей, но эти изменения не будут сохраняться при перезагрузках. Для внесения постоянных изменений в учетные записи пользователей следует использовать интерфейс командной строки Numa Edge.

5.1.2 Интерфейс командной строки и интерпретатор команд системы Numa Edge

В интерфейсе командной строки системы имеются команды двух типов:

- специфичные команды для эксплуатации и настройки системы Numa Edge;
- команды, предоставляемые интерпретатором команд операционной системы, в котором работает интерфейс командной строки Numa Edge.

Команды, которые может выполнить пользователь, зависят от его роли. Однако любая команда, которую пользователь может выполнить, может быть запущена из интерфейса командной строки Numa Edge.

5.1.3 Уровни полномочий пользователя

Numa Edge поддерживает две роли пользователей:

- Администратор;
- Оператор.

Роль «Администратор»

Административные пользователи имеют полный доступ к интерфейсу командной строки Numa Edge. Административные пользователи могут просматривать, настраивать и удалять информацию, а также выполнять все эксплуатационные команды Numa Edge. Кроме того, административные пользователи могут выполнять все команды и конструкции интерпретатора команд операционной системы.

Не рекомендуется использовать команды ОС. При их использовании корректная работоспособность системы не гарантируется.

Пользователь по умолчанию `admin` является административным пользователем.

Для создания административного пользователя необходимо выполнить следующую последовательность команд в режиме настройки:

```
[edit]
admin@edge# set system login user имя_пользователя level admin
```

```
[edit]
admin@edge# set system login user имя_пользователя authentication plaintext-
password пароль
[edit]
admin@edge# commit
```

где имя_пользователя - идентификатор создаваемой учетной записи, а *пароль* – пароль, назначаемый указанному пользователю (пароль должен соответствовать требованиям к устанавливаемому паролю).

Несмотря на то, что команды интерпретатора команд операционной системы доступны административному пользователю всегда, они не отображаются при использовании этими пользователями автодополнения команд для запроса доступных команд у интерфейса командной строки. Это происходит по той причине, что в любой момент доступно несколько сот команд и конструкций интерпретатора команд операционной системы: если показывать все доступные команды интерпретатора команд операционной системы, то различить доступные команды интерфейса командной строки Numa Edge будет очень сложно.

Административные пользователи могут просмотреть доступные команды, введя help в запросе для ввода команд.

Роль «Оператор»

Пользователям-операторам предоставлен доступ только на чтение конфигурации и возможность выполнения эксплуатационных команд Numa Edge. Пользователи-операторы могут выполнять просмотр в эксплуатационном режиме (при помощи команд show), настраивать параметры своих терминалов (при помощи команды terminal), а также выходить из интерфейса командной строки Numa Edge (при помощи команды exit). Но не могут входить в режим настройки, однако они могут отображать конфигурацию при помощи команды show configuration в эксплуатационном режиме. Им доступны основные команды для отображения сведений (например, show configuration, а также конвейер "|" и такие команды как more или less, для управления выводом на экран). Команды, в которых используются конструкции для контроля за порядком выполнения (такие как if, for и т.д.), операции для списков (такие как ";", "&&" и т.д.) и перенаправление, недоступны для пользователей-операторов.

Для создания пользователя-оператора необходимо выполнить следующую последовательность команд в режиме настройки:

```
[edit]
admin@edge# set system login user имя_пользователя level operator
[edit]
admin@edge# set system login user имя_пользователя authentication plaintext-
password пароль
[edit]
admin@edge# commit
```

где имя_пользователя - идентификатор создаваемой учетной записи, а пароль – пароль, назначаемый указанному пользователю (пароль должен соответствовать требованиям к устанавливаемому паролю).

Команды интерпретатора команд операционной системы недоступны пользователям-операторам, соответственно, список команд, выдаваемых автодополнением команд пользователям уровня оператора, ограничен командами Numa Edge.

5.1.4 Режимы интерфейса

В интерфейсе командной строки Numa Edge имеются два режима:

- эксплуатационный режим;
- режим настройки.

В эксплуатационном режиме обеспечивается доступ к эксплуатационным командам для отображения и очистки сведений, включения или выключения отладки, настройки параметров терминалов, а также перезагрузки и выключения системы.

В режиме настройки обеспечивается доступ к командам для создания, изменения, удаления, фиксации изменений, загрузки и сохранения конфигурации, а также отображения сведений о конфигурации, и для переходов по иерархии конфигурации.

При входе в систему она находится в эксплуатационном режиме.

Для входа из эксплуатационного режима в режим настройки используется команда `configure`.

Для возврата из режима настройки в эксплуатационный режим используется команда `exit`. Если имеются незафиксированные изменения в конфигурации, их следует или зафиксировать с помощью команды `commit`, или отменить с помощью команды `discard` (или команды `exit discard`) перед тем, как можно будет выйти в эксплуатационный режим.

При выполнении команды `exit` в эксплуатационном режиме происходит выход из системы.

5.1.5 Запросы для ввода команд

Запрос для ввода команд показывает пользователю:

- имя учетной записи пользователя под которой выполнен вход в систему;
- имя узла системы, на который выполнен вход;
- текущий режим интерфейса командной строки;
- текущий уровень в иерархии конфигурации (только для режима настройки).

В таблице приведены некоторые примеры запросов на ввод команд и их значения.

Таблица 2– Запросы на ввод команд

Вид запроса	Описание запроса
`admin@edge:~$`	Пользователь: admin Имя узла: edge Режим интерфейса: эксплуатационный режим
`[edit]` `admin@edge#`	Пользователь: admin Имя узла: edge Режим интерфейса: режим настройки Уровень в иерархии конфигурации: [edit] (верхний уровень)

5.1.6 Использование специальных символов в командах

Интерфейс командной строки Numa Edge основан на интерпретаторе команд bash проекта GNU. При вводе команды в запросе следует иметь в виду, что некоторые символы имеют специальное значение для интерпретатора. Например, одним из таких специальных символов является символ пробела, который обозначает конец лексемы в команде, как показано ниже:

```
admin@edge# show system login
```

В данном примере символы пробела разделяют командную строку на три компоненты: "`show`", "`system`" и "`login`".

При необходимости ввода строки с литеральным символом, воспринимаемый интерпретатором команд как специальный символ, необходимо заключить этот символ в кавычки. Например, если необходимо ввести строку с пробелом, необходимо заключить ее в кавычки, как показано ниже:

```
admin@edge# set system login user backup full-name "User for backup"
```

В данном примере пробел внутри строки "`User for backup`" заключен в кавычки и поэтому теряет свое специальное значение как разделитель лексем.

Другой пример специального символа - это символ конвейера (называемый также вертикальной чертой, "|"), который разделяет две команды и означает, что вывод команды слева от вертикальной черты будет обработан командой справа от вертикальной черты, как показано в следующем примере:

```
admin@edge# show system login | grep user
```

В данном примере символ конвейера указывает интерпретатору команд выполнить команду `show system login` и затем обработать ее вывод с помощью команды `grep user`. В результате будут отображены только строки, содержащие строку "`user`".

Как и в случае символа пробела, если в качестве компонента команды необходим литеральный символ вертикальной черты, следует заключить его в кавычки.

Помимо пробела и вертикальной черты, специальное значение для интерпретатора команд имеют следующие символы:

- амперсанд ("&");
- точка с запятой (";");
- запятая (",");
- левая скобка ("(");
- правая скобка (")");
- знак "меньше" ("<");
- знак "больше" (">");
- обратная косая черта ("\");
- диез ("#").

При отсутствии уверенности в том, какие именно символы являются специальными, следует взять за правило заключать в кавычки всё, что не является алфавитно-цифровыми символами.

Рекомендуется не использовать символы кавычек и обратной косой черты в качестве литеральных значений в конфигурации.

5.1.7 Автодополнение команд

Интерпретатор команд системы Numa Edge поддерживает автодополнение команд. Для автоматического завершения синтаксиса команды или вывода подсказки системой следует ввести в запросе на ввод командной строки любой из элементов, приведенных в таблице.

Таблица 3 – Справочные клавиши интерфейса командной строки

Клавиша/Сочетание	**Функция**
<Tab>	При первом нажатии клавиши <Tab>: если ввод осуществляется непосредственно после приглашения командной строки, либо после предыдущей лексемы, то система отобразит все доступные команды текущего уровня иерархии; Обратите внимание, что пробел после команды или ключевого слова считается за лексему. если введен(ы) первый(е) символ(ы) команды и команда однозначна, то система выполнит автодополнение команды и автоматически создаст следующую лексему в синтаксисе. Если возможен более чем один вариант автодополнения, то система отобразит список возможных последующих лексем. При втором нажатии клавиши <Tab> система отобразит справку интерфейса командной строки для текущего списка лексем.
<Shift>+<?>	При первом нажатии сочетания клавиш <Shift>+<?>: если ввод осуществляется непосредственно после приглашения командной строки, либо после предыдущей лексемы, то система отобразит все доступные команды текущего уровня иерархии; Обратите внимание, что пробел после команды или ключевого слова считается за лексему. если введен(ы) первый(е) символ(ы) команды и команда однозначна, то система отобразит полное наименование лексемы. Если возможен более чем один вариант

Клавиша/Сочетание	Функция
	автодополнения, то система отобразит список возможных последующих лексем. Для ввода литерального вопросительного знака необходимо вначале ввести <Ctrl>+<v>, а затем вопросительный знак. При втором нажатии сочетания клавиш <Shift>+<?> система отобразит справку интерфейса командной строки для текущего списка лексем.

В следующем примере осуществляется поиск всех доступных команд.

```
admin@edge:~$ <Tab>
```

В следующем примере запрашивается завершение команды для набранной строки "`conf`". В данном примере завершение команды однозначно.

```
admin@edge:~$ conf<Tab>
admin@edge:~$ configure
```

В следующем примере запрашивается завершение команды для набранной строки "`c`". В текущем случае ввод может быть завершен более чем одним способом, и система выдает все допустимые варианты завершения.

```
admin@edge:~$ c<Tab>
clear      configure  connect
```

Обратите внимание, что ни клавиша <Tab>, ни сочетание клавиш <Shift>+<?> не обеспечивают функцию справки по командам, если заключены в кавычки.

5.1.8 Журнал команд

Интерпретатор команд системы Numa Edge поддерживает журнал команд, хранящий во внутреннем буфере выполненные команды, которые можно выполнить повторно или исправить.

В таблице показаны наиболее важные сочетания клавиш для работы с журналом команд.

Таблица 4– Сочетания клавиш для работы с журналом команд

Клавиша/Сочетание	Функция
<Стрелка_вверх> <Control>+<p>	Переход к предыдущей команде.
<Стрелка_вниз> <Control>+<n>	Переход к следующей команде.

5.1.9 Правка команд

Интерпретатор команд системы Numa Edge поддерживает правку команд в стиле emacs. В таблице приведены наиболее важные сочетания клавиш для правки.

Таблица 5 – Сочетания клавиш для правки команд в командной строке

Клавиша/Сочетание	Функция
<Стрелка_влево> <Control>+<b>	Перемещение на один символ назад в командной строке.
<Стрелка_вправо> <Control>+<f>	Перемещение на один символ вперед в командной строке.
<Control>+<a>	Перемещение в начало командной строки.
<Control>+<e>	Перемещение в конец командной строки.

Клавиша/Сочетание	Функция
<Control>+<d>	Удаление символа непосредственно под курсором.
<Control>+<t>	Перестановка местами символа под курсором и символа, непосредственно ему предшествующего.
<Control>+<Space>	Отметка текущего положения курсора.
<Control>+<w>	Удаление текста между отметкой и текущим положением курсора с копированием удаленного текста в буфер обмена.
<Control>+<k>	Удаление текста от курсора до конца строки с копированием удаленного текста в буфер обмена.
<Control>+<y>	Вставка текста из буфера обмена в командную строку от положения курсора.

5.1.10 Фильтрация вывода команд

В системе Numa Edge можно передать по конвейеру вывод команд на вход определенных команд интерпретатора команд операционной системы для фильтрации сведений, отображаемых на консоли. Конвейер от команд к фильтрам организуется с помощью знака операции "вертикальная черта" ("|").

В таблице показаны команды конвейера, реализованные в системе Numa Edge.

Таблица 6 – Команды конвейерной фильтрации

Сочетание	Функция
count	Подсчет экземпляров.
match *шаблон*	Отобразить только текст, соответствующий указанному шаблону.
more	Постраничный вывод.
no-match *шаблон*	Отобразить только текст, не соответствующий указанному шаблону.
no-more	Не использовать постраничный вывод.

5.1.11 Отображение длинного вывода

Если отображаемые сведения слишком длинны и не помещаются на один экран, то отображение приостанавливается по выдаче одного экрана и в месте разрыва вывода появляется отметка "More" или ":".

В таблице показаны сочетания клавиш для управления отображением сведений на экране "More".

Таблица 7– Варианты отображения на экране "More"

Клавиша/Сочетание	Функция
<q> <Q>	Выход из экрана "More".
<Пробел> <f> <Ctrl>+<f>	Пролистывание целого экрана вниз.
<b> <Ctrl>+<b>	Пролистывание целого экрана вверх.
<d> <Ctrl>+<d>	Пролистывание половины экрана вниз.
<u> <Ctrl>+<u>	Пролистывание половины экрана вверх
<Enter> <e> <Ctrl>+<e> <Стрелка_вниз>	Пролистывание строки вниз.
<y> <Ctrl>+<y> <Стрелка_вверх>	Пролистывание строки вверх.
<G>	Пролистывание вниз до конца вывода.
<g>	Пролистывание вверх до начала вывода.
<h>	Отображение подробной справки для функции "More".

Клавиша/Сочетание	Функция
<H>	

5.1.12 Работа с конфигурацией

О возможности одновременного редактирования конфигурации

ПРЕДУПРЕЖДЕНИЕ Система конфигурирования Numa Edge не обеспечивает возможности одновременного редактирования конфигурации. К таким ситуациям относятся:

- Одновременное редактирование конфигурации несколькими пользователями.
- Одновременное редактирование конфигурации различными способами подключения (доступ к интерфейсу командной строки через последовательный порт, подключение по SSH, использование web-интерфейса).

В случаях, когда вероятна ситуация одновременной работы с конфигурацией, в первую очередь перед внесением изменений следует воспользоваться командой конфигурационного режима `show`. Если вы видите, что большая часть конфигурации устройства помечена на удаление, значит конфигурация была изменена в другой сессии. В таком случае предварительно следует выполнить команду `discard`.

Вход в режим настройки и выход из него

Для входа в режим настройки необходимо выполнить команду `configure` в эксплуатационном режиме:

```
admin@edge:~$ configure
[edit]
admin@edge#
```

Вид запроса на ввод команд изменяется в зависимости от режима:

- вид запроса в эксплуатационном режиме:

```
пользователь@узел:~$
```

- вид запроса в режиме настройки:

```
пользователь@узел#
```

Для выхода из режима настройки с верхнего уровня иерархии конфигурации используется команда `exit`.

Если конфигурация изменена, то необходимо либо зафиксировать изменения с помощью команды `commit`, либо отменить их с помощью команды `exit discard`.

Иерархия конфигурации

В Numa Edge используется иерархическая система команд. Для того чтобы изменить некоторый параметр системы, необходимо задать значение для соответствующего атрибута. Конфигурация Numa Edge упорядочена в виде иерархии, аналогичной структуре файловой системы UNIX. Узлы конфигурации (подобно каталогам файловой системы) могут включать в себя другие узлы, а также атрибуты (подобны файлам в ФС), которые позволяют установить значения или характеристики для параметров внутри узла.

Узел конфигурации всегда включает закрытую пару фигурных скобок, содержимое которой может как отсутствовать:

```
firewall Drop_policy {
}
```

так и присутствовать:

```
firewall Accept_policy {
    default-action accept
    description "Firewall Accept Policy"
}
```

Атрибут конфигурации имеет вид *атрибут значение*, например, как в приведенном ниже примере.

```
default-action accept
```

Узлы конфигурации и атрибуты формируют *ветви* конфигурации, как показано на рисунке ниже.

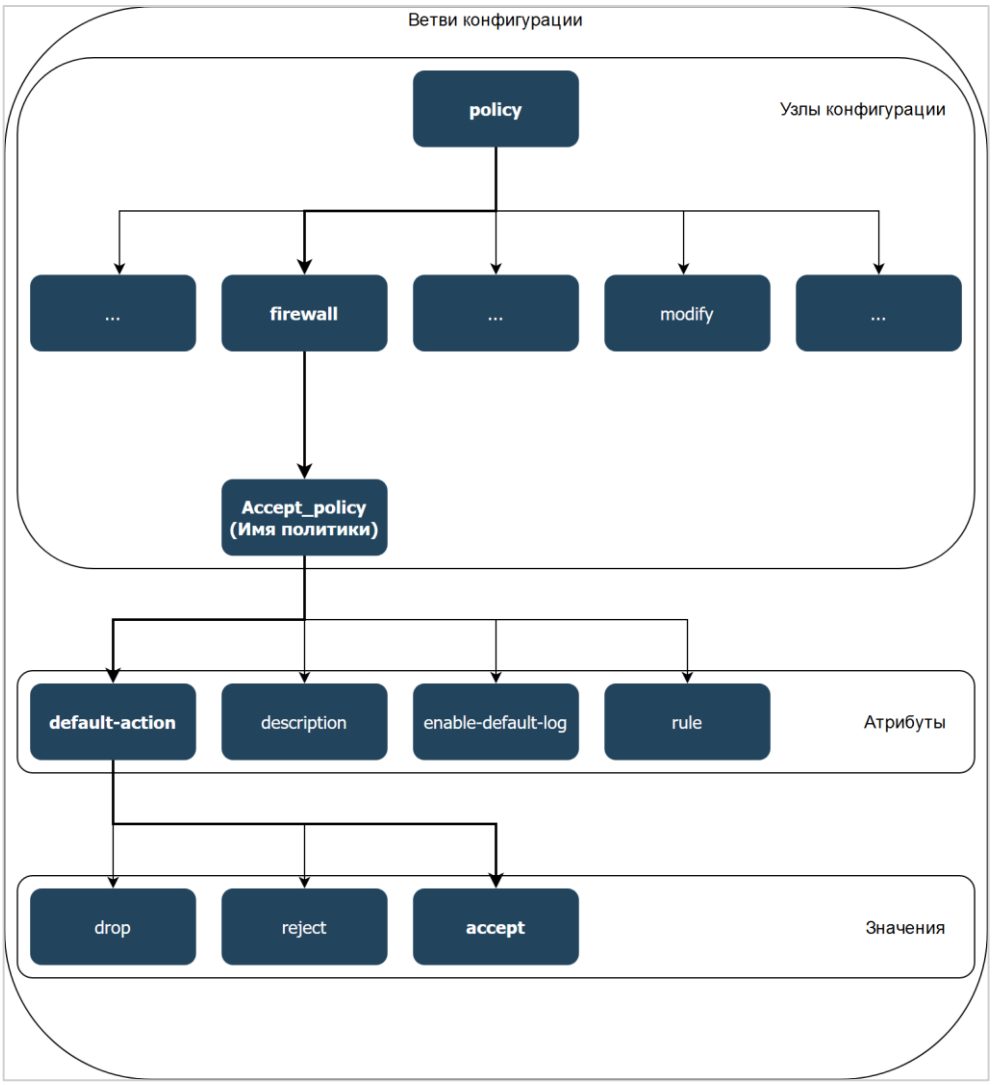


Рисунок 1 – Иерархия конфигурации

Местоположение в конфигурации можно определить по запросу в квадратных скобках, указывающему текущий уровень иерархии в конфигурации.

На верхнем уровне иерархии запрос отображается следующим образом:

```
[edit]
```

При нахождении в другом месте в запросе отображается текущее местоположение путем вывода иерархии узлов в порядке их следования, например:

```
[edit policy firewall Accept_policy]
```

Для того чтобы задать значение для некоторого атрибута, необходимо указывать путь к атрибуту в конфигурации относительно текущего уровня иерархии (указывать все узлы конфигурации в ветви конфигурации до требуемого атрибута). Пример перехода между уровнями иерархии конфигурации приведен на рисунке ниже.

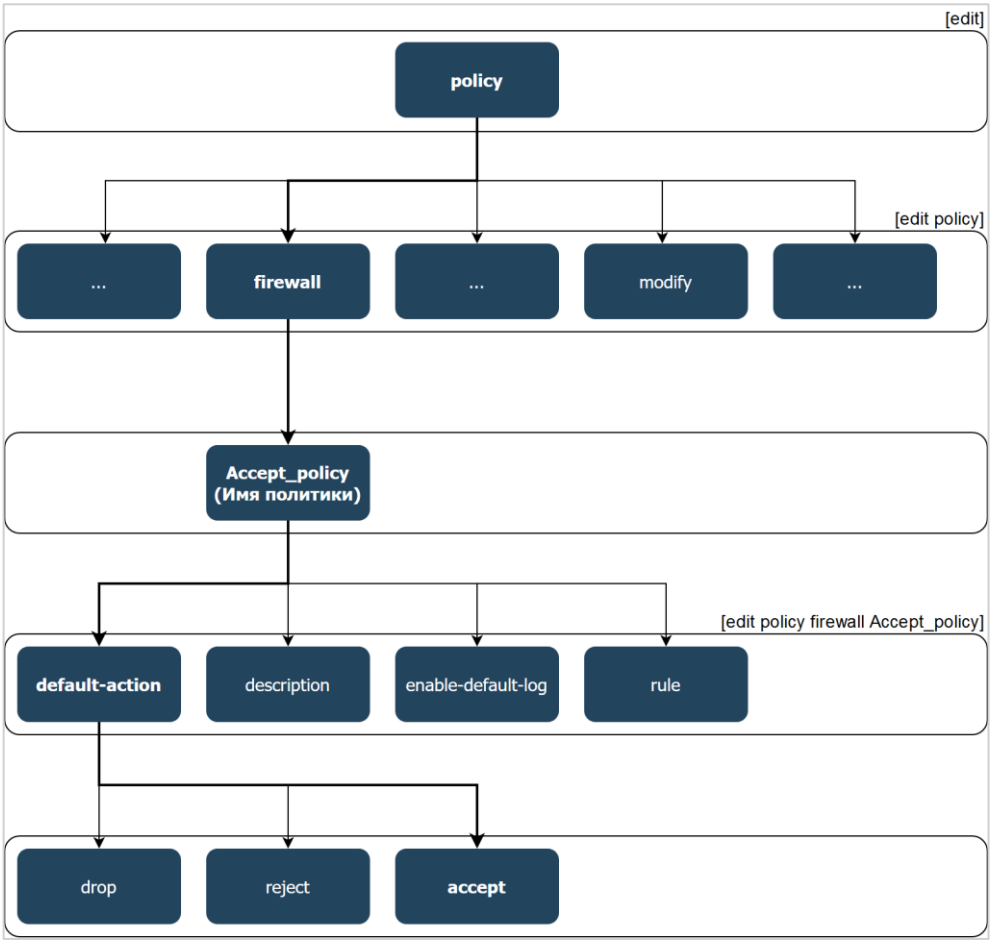


Рисунок 2 – Пример перехода между уровнями иерархии конфигурации

Например, чтобы, находясь на верхнем уровне иерархии, указать в качестве действия по умолчанию для политики межсетевого экрана `Accept_policy` пропускать пакеты протокола IPv4, необходимо ввести следующую команду:

```
[edit]
admin@edge# set policy firewall Accept_policy default-action accept
```

В случае если установлен текущий уровень иерархии `[edit policy firewall Accept_policy]`, то для установки значения необходимо ввести команду:

```
[edit policy firewall Accept_policy]
admin@edge# set default-action accept
```

В таблице ниже показаны команды для переходов в режиме настройки.

Таблица 8 – Команды для переходов в режиме настройки

Команда	**Результат**
edit узел_конфигурации	Переход к указанному узлу конфигурации для внесения изменений. К моменту фиксации изменений в конфигурации узел уже должен быть создан.
exit	Переход к вершине дерева конфигурации. При нахождении на вершине дерева конфигурации - выход из режима настройки и возвращение в эксплуатационный режим.
top	Переход к вершине дерева конфигурации.

Команда	Результат
up	Перемещение на один узел вверх в дереве конфигурации.

Команда `edit` позволяет переходить в интересующую пользователя часть иерархии и выполнять команды относительно местоположения. Это позволяет сократить набор в командной строке при необходимости работы в конкретной части иерархии.

Узлы и атрибуты могут быть одиночными (в конфигурации может быть создан один экземпляр) и множественными (может быть создано более одного экземпляра).

Множественные атрибуты используются для задания списка значений параметра. Большинство атрибутов допускает установку только одного значения. Для установки нескольких значений атрибута, где это допускается, следует вводить их с использованием последовательности команд. Например, для указания политике модификации трафика `Modify_policy` удалять из пакета данные о максимальном размере сегмента (`mss`), временной отметке (`timestamp`) и масштабировании окна (`wscale`), необходимо ввести следующую последовательность команд:

```
[edit]
admin@edge# set policy modify Modify_policy rule 10 strip tcp-option mss
[edit]
admin@edge# set policy modify Modify_policy rule 10 strip tcp-option timestamp
[edit]
admin@edge# set policy modify Modify_policy rule 10 strip tcp-option wscale
```

Параметры, допускающие многократный ввод и сохранение разных значений, называются «множественными», так как в конфигурации Numa Edge они будут созданы как однотипные узлы на одном уровне иерархии, различающиеся только своими значениями:

```
[edit]
admin@edge# show policy modify
   Modify_policy {
        rule 10 {
            strip {
                tcp-option mss
                tcp-option timestamp
                tcp-option wscale
            }
        }
   }
```

Просмотр конфигурации

Команда `show` в режиме настройки используется для отображения конфигурации. Вывод команды можно ограничить отображением конкретного узла, указав путь к нему.

В приведенном ниже примере отображается конфигурация для всех настроенных правили маршрутизации.

```
[edit]
admin@edge# show policy firewall
   Accept_policy {
        default-action accept
        description "Firewall Accept Policy"
   }
   Drop_policy {
        default-action drop
   }
```

В приведенном ниже примере отображается конфигурация только для политики межсетевого экрана `Drop_policy`.

```
[edit]
```

```
admin@edge# show policy firewall Drop_policy
   default-action drop
```

Добавление в конфигурацию или изменение конфигурации

Добавление в конфигурацию выполняется с помощью создания узла конфигурации командой `set` в режиме настройки, как в приведенном ниже примере:

```
[edit]
admin@edge# set policy firewall New_policy default-action reject
```

Для просмотра изменений можно использовать команду `show`:

```
[edit]
admin@edge# show policy firewall
  +New_policy {
  +    default-action reject
  +}
```

Обратите внимание на знак “+” перед новым узлом и/или атрибутом настройки. Он показывает, что узел/атрибут был добавлен в конфигурацию, но изменение еще не зафиксировано. Изменение не вступает в силу до тех пор, пока конфигурация не будет зафиксирована с помощью команды `commit`.

Изменение существующей конфигурации так же выполняется с помощью команды `set` в режиме настройки, как в приведенном ниже примере:

```
[edit]
admin@edge# set policy firewall New_policy default-action drop
```

Для просмотра изменений можно использовать команду `show`:

```
[edit]
admin@edge# show policy firewall
   New_policy {
  >    default-action drop
   }
```

Обратите внимание на знак “>” перед измененным узлом и/или атрибутом настройки. Он показывает, что узел/атрибут был изменен в конфигурации, но изменение еще не зафиксировано. Изменение не вступает в силу до тех пор, пока конфигурация не будет зафиксирована с помощью команды `commit`.

Конфигурацию можно изменять начиная с корня дерева конфигурации или использовать команду `edit` для перемещения к части дерева, в которой необходимо выполнить изменения или добавления.

При первой загрузке системы дерево конфигурации содержит только нескольких автоматически настроенных узлов. Для любой функциональности, которую нужно настроить в системе, необходимо создать узел. При создании узла, к нему применяются все значения по умолчанию для его атрибутов.

Удаление конфигурации

Для удаления атрибута или целого узла в конфигурации используется команда `delete`. В приведенном ниже примере выполняется удаление описания политики межсетевого экрана:

```
[edit]
admin@edge# delete policy firewall New_policy description "New Policy
Firewall"
```

Для просмотра изменений можно использовать команду `show`:

```
[edit]
```

```
admin@edge# show policy firewall
   New_policy {
       default-action reject
  -    description "New Policy Firewall"
   }
```

Обратите внимание на знак “-” перед удаленным узлом и/или атрибутом настройки. Он показывает, что узел/атрибут был удален из конфигурации, но изменение еще не зафиксировано. Изменение не вступает в силу до тех пор, пока конфигурация не будет зафиксирована с помощью команды `commit`.

Некоторые узлы конфигурации являются обязательными и их нельзя удалить. Некоторые узлы конфигурации являются обязательными, но имеют значения по умолчанию; при удалении одного из таких узлов будет восстановлено значение по умолчанию.

Клонирование узла конфигурации

Для экономии времени при вводе информации можно копировать (или клонировать) множественные узлы конфигурации. Множественные узлы конфигурации (узлы, допускающие несколько экземпляров) отличаются друг от друга по идентификаторам. Например, у правил межсетевого экрана и NAT есть номера, у наборов правил межсетевого экрана есть имена, у планов IPSec в VPN есть имена, у пользователей системы есть идентификаторы пользователей.

В приведенном ниже примере выполняется клонирование правила `10` фильтра трафика `LAN_filter` с указанием нового номера правила `30`.

Для клонирования узла конфигурации необходимо с помощью команды `edit` перейти в точку иерархии конфигурации сразу над узлом, который необходимо скопировать. В текущем примере выполнен переход в фильтр `LAN_filter`:

```
[edit]
admin@edge# edit filter LAN_filter
```

Далее для выполнения клонирования узла использовать команду `copy`:

```
[edit filter LAN_filter]
admin@edge# copy rule 10 to rule 30
```

где `rule 10` - копируемое правило, `rule 30` - новое правило.

Результат выполнения приведенной выше команды:

```
[edit filter LAN_filter]
admin@edge# show
   rule 10 {
       description "Rule 10"
       source {
           address 192.168.10.0/24
       }
   }
  +rule 30 {
  +    description "Rule 10"
  +    source {
  +        address 192.168.10.0/24
  +    }
  +}
```

Переименование узлов конфигурации

Следует учесть, что с помощью команды `set` нельзя изменить идентификатор узла, у которого может быть несколько экземпляров (“множественный узел”), такого как сервер DNS или IP-адрес интерфейса. Однако идентификатор множественного узла можно изменить с помощью команды `rename`.

Для переименования узла конфигурации необходимо с помощью команды `edit` перейти в точку иерархии конфигурации сразу над узлом, который необходимо переименовать. Далее командой `rename` изменить идентификатор. В приведенном ниже примере выполняется переименование правила `30` фильтра трафика `LAN_filter` с указанием нового номера правила `50`.

```
[edit filter LAN_filter]
admin@edge# rename rule 30 to rule 50
```

Результат выполнения приведенной выше команды:

```
[edit filter LAN_filter]
admin@edge# show
   rule 10 {
       description "Rule 10"
       source {
           address 192.168.10.0/24
       }
   }
  -rule 30 {
  -    description "Rule 10"
  -    source {
  -        address 192.168.10.0/24
  -    }
  -}
  +rule 50 {
  +    description "Rule 10"
  +    source {
  +        address 192.168.10.0/24
  +    }
  +}
```

Фиксация изменений в конфигурации

В Numa Edge изменения в конфигурации не вступают в силу до тех пор, пока они не зафиксированы с помощью команды `commit`.

```
[edit]
admin@edge# commit
```

Незафиксированные изменения помечаются либо знаком плюс “+” (в случае добавления или изменения) или минус “-” (в случае удаления). При фиксации изменений знаки удаляются, как в приведенном ниже примере:

```
[edit]
admin@edge# show policy firewall
   New_policy {
       default-action reject
  +    description "New Policy Firewall"
   }
[edit]
admin@edge# commit
[edit]
admin@edge# show policy firewall
   New_policy {
       default-action reject
       description "New Policy Firewall"
   }
```

Отмена изменений в конфигурации

Выйти из режима настройки при наличии незафиксированных изменений невозможно:

```
[edit]
admin@edge# exit
Cannot exit: configuration modified.
Use 'exit discard' to discard the changes and exit.
```

Необходимо либо зафиксировать изменения, либо отказаться от них. Если фиксировать изменения не нужно, можно отменить их с помощью команды `exit discard`:

```
[edit]
admin@edge# exit discard
exit
admin@edge:~$
```

Сохранение конфигурации

Работающую конфигурацию можно сохранить при помощи команды `save` в режиме настройки. По умолчанию, конфигурация сохраняется в файл `config.boot` в стандартном каталоге конфигурации, которым является `/etc/config`.

```
[edit]
admin@edge# save
Запись конфигурации в '/etc/config/config.boot'...
Готово
```

Конфигурация может быть сохранена под другим именем в каталог `/etc/config`:

```
[edit]
admin@edge# save backupconfig
Запись конфигурации в '/etc/config/backupconfig'...
Готово
```

Так же конфигурацию можно сохранить на жесткий диск по пути, отличающемуся от стандартного каталога `/etc/config`, внешний накопитель (например, USB-флеш-накопителя), удаленное устройство по протоколам FTP, TFTP, SCP или HTTP. Перед тем, как конфигурацию можно будет сохранить на флэш-накопитель, последний следует проинициализировать командой `flash init` в эксплуатационном режиме.

Обратите внимание, что команда `save` записывает только зафиксированные изменения.

Загрузка сохраненной конфигурации

Для загрузки ранее сохраненной конфигурации используется команда `load` в режиме настройки. По умолчанию система считывает файл из стандартного каталога конфигурации. По умолчанию это каталог `/etc/config`.

```
[edit]
admin@edge# load backupconfig
Loading configuration from '/etc/config/backupconfig'...
Done
```

Загруженная конфигурация автоматически фиксируется и становится активной конфигурацией.

Так же конфигурацию можно загрузить с жесткого диска по пути, отличающемуся от стандартного каталога `/etc/config`, внешнего накопителя (например, USB-флеш-накопителя), удаленного устройства по протоколам FTP, TFTP, SCP или HTTP.

5.1.13 Выполнение эксплуатационной команды из режима настройки

С помощью команды `run` можно выполнить эксплуатационную команду, не выходя из режима настройки, как в приведенном ниже примере:

```
[edit]
admin@edge# run policy show firewall Accept_policy
Политика МЭ IPv4 Accept_policy:

 Политика не задействована ни для одного интерфейса, туннеля или зоны.


rule      pkts      bytes     target    filter
----      ----      -----     ------    ------
default   0         0         ACCEPT
```

5.1.14 Отображение конфигурации из эксплуатационного режима

При помощи команды `show configuration` можно отобразить сведения о конфигурации, не выходя из эксплуатационного режима, как в приведенном ниже примере:

```
admin@edge:~$ show configuration
...
  filter LAN_filter {
      rule 10 {
          description "Rule 10"
          source {
              address 192.168.10.0/24
          }
      }
      rule 50 {
          description "Rule 10"
          source {
              address 192.168.10.0/24
          }
      }
  }
  policy {
      firewall Accept_policy {
          default-action accept
          description "Firewall Accept Policy"
      }
      firewall Drop_policy {
          default-action drop
      }
      firewall New_policy {
          default-action reject
          description "New Policy Firewall"
      }
      modify Modify_policy {
          rule 10 {
              strip {
                  tcp-option mss
                  tcp-option timestamp
                  tcp-option wscale
              }
          }
      }
  }
...
```

5.2 Основные команды интерфейса командной строки

Основные команды интерфейса командной строки

Команды настройки

Команды настройки	
commit	Применение любых незафиксированных изменений в конфигурации.
copy	Копирование или клонирование узла конфигурации.
delete	Удаление узла конфигурации.
discard	Отмена любых незафиксированных изменений в конфигурации.
edit	Переход к подузлу дерева конфигурации для правки.
exit	Переход на один уровень использования выше.
load	Загрузка сохраненной конфигурации.
loadkey	Загрузка пользовательского ключа SSH из файла.
merge	Слияние сохраненной конфигурации с активной (работающей) конфигурацией.
rename	Изменение идентификатора именованного узла конфигурации.
run	Выполнение эксплуатационной команды без выхода из режима настройки.
save	Сохранение работающей конфигурации в файл.
set	Создание нового узла конфигурации или изменение значения в существующем узле конфигурации.
show	Отображение сведений о конфигурации в режиме настройки.
top	Перемещение на верхний уровень иерархии конфигурации.
up	Перемещение на уровень вверх в дереве конфигурации.
Эксплуатационные команды	
configure	Вход в режим настройки.
exit	Переход на один уровень использования выше.
show configuration	Отображение конфигурации системы из эксплуатационного режима.

5.2.1 commit

Применение любых незафиксированных изменений в конфигурации.

Синтаксис

```
commit
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

Отсутствует.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для применения изменений конфигурации.

При добавлении какого-либо параметра в конфигурацию, изменении существующей конфигурации или удалении конфигурации из системы сделанные изменения должны быть зафиксированы, после чего они вступят в силу. Для фиксации изменений используется команда `commit`.

При попытке выхода из режима настройки или выхода из системы при наличии незафиксированных изменений в конфигурации система выдаст предупреждение. Выйти из режима настройки будет невозможно до фиксации изменений с помощью команды `commit` или отказа от изменений с помощью команды `exit discard`.

До тех пор, пока изменение конфигурации не зафиксировано, при отображении сведений система помечает его.

Фиксация сведений может занять некоторое время в зависимости от сложности настройки и занятости системы. Будьте готовы к нескольким секундам ожидания завершения процесса фиксации изменений системой. Если в систему вошли двое или больше пользователей, и один из них изменяет конфигурацию, другие получат предупреждение.

Примеры

В примере показано незафиксированное удаление, которое затем фиксируется. В этом примере обратите внимание, что незафиксированное удаление помечено знаком минуса ("-"), который исчезает после фиксации.

Пример 1 – Фиксация изменений в конфигурации

```
[edit]
admin@edge# show interfaces ethernet eth2
 -address 192.168.1.100/24
[edit]
admin@edge# commit
[edit]
admin@edge# show interfaces ethernet eth2
[edit]
admin@edge#
```

5.2.2 copy

Копирование или клонирование узла конфигурации.

Синтаксис

```
copy <исходный_узел_конф> to <конечный_узел_конф>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

Отсутствует.

Параметры

исходный_узел_конф

Узел конфигурации, который требуется скопировать. Формат представляет собой последовательность разделенных пробелами лексем, представляющих имя параметра конфигурации и значение этого параметра; например, `rule правило_1`.

конечный_узел_конф

Узел конфигурации, который требуется создать. Формат представляет собой последовательность разделенных пробелами лексем, представляющих имя параметра конфигурации и значение этого параметра; например, `rule правило_2`.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для создания копии (клона) подузла конфигурации. Допустимо копирование только тех узлов, которые расположены на текущем редактируемом уровне конфигурации. Текущий уровень конфигурации отображается в квадратных скобках над строкой-приглашением ко вводу команд, например, `[edit policy firewall]`. Для перехода на нужный уровень конфигурации, следует использовать команду `edit`. Команда `edit` используется для перехода к нужному месту в иерархии конфигурации, после чего выполняется копирование нужного подузла.

Если вывести конфигурацию до ее фиксации, можно увидеть, что скопированный узел помечен знаком плюс (“+”). Данная пометка исчезает после фиксации изменения в конфигурации.

Примеры

В примере выполняется копирование правила `10` в политике межсетевого экрана `RULE-SET-1`.

Пример 2– Клонирование подузлов конфигурации

```
[edit]
admin@edge# show policy firewall
   RULE-SET-1 {
       rule 10 {
           action accept
       }
   }
[edit]
admin@edge# edit policy firewall RULE-SET-1
[edit policy firewall RULE-SET-1]
admin@edge# copy rule 10 to rule 20
[edit policy firewall RULE-SET-1]
admin@edge# show
   rule 10 {
       action accept
   }
  +rule 20 {
  +    action accept
  +}
[edit policy firewall RULE-SET-1]
admin@edge# commit
[edit policy firewall RULE-SET-1]
admin@edge# show
   rule 10 {
       action accept
   }
   rule 20 {
       action accept
   }
[edit policy firewall RULE-SET-1]
admin@edge# top
[edit]
admin@edge#
```

5.2.3 delete

Удаление узла конфигурации.

Синтаксис

```
delete <узел_конфигурации>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

Отсутствует.

Параметры

узел_конфигурации

Узел конфигурации, который следует удалить, в том числе полный путь в иерархии конфигурации в виде последовательности лексем, разделенных пробелами.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для удаления части конфигурации. Для этого удаляется нужный подузел узла конфигурации.

Если вывести конфигурацию до ее фиксации, можно увидеть, что удаленный узел и/или атрибут помечен знаком минус ("-"). Данная пометка исчезает после фиксации изменения в конфигурации.

Некоторые узлы конфигурации являются обязательными и их нельзя удалить. Некоторые узлы конфигурации являются обязательными, но имеют значения по умолчанию; при удалении одного из таких узлов будет восстановлено значение по умолчанию.

Примеры

В примере выполняется удаление сервера DNS из конфигурации системы.

Пример 3– Удаление конфигурации

```
[edit]
admin@edge# show system dns name-server
   192.168.10.40 {
   }
   192.168.10.41 {
   }
   192.168.10.42 {
   }
[edit]
admin@edge# delete system dns name-server 192.168.10.41
[edit]
admin@edge# show system dns name-server
   192.168.10.40 {
   }
  -192.168.10.41 {
  -}
   192.168.10.42 {
   }
```

5.2.4 discard

Отмена любых незафиксированных изменений в конфигурации.

Синтаксис

```
discard
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

Отсутствует.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отмены всех незафиксированных изменений в конфигурации.

Примеры

В примере показано незафиксированное удаление и незафиксированное добавление, которые затем отменяются. В этом примере обратите внимание, что незафиксированное удаление (помеченное знаком минус "-") и незафиксированное добавление (помеченное знаком плюс "+") исчезают после вызова команды `discard`.

Пример 4– Отмена изменений в конфигурации

```
[edit]
admin@edge# show interfaces ethernet eth1
  -address 192.168.10.254/24
  +address 192.168.10.1/24
[edit]
admin@edge# discard
Changes have been discarded
[edit]
admin@edge# show interfaces ethernet eth1
   address 192.168.10.254/24
```

5.2.5 edit

Переход к подузлу дерева конфигурации для правки.

Синтаксис

```
edit <путь>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

Отсутствует.

Параметры

путь

Путь к узлу дерева конфигурации, который нужно править.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для перехода к конкретному подузлу конфигурации для правки. Запрос `[edit]` динамически изменяется, отражая положение пользователя в дереве конфигурации. В текущем местоположении любые выполняемые действия, такие как отображение, создание или удаление конфигурации, выполняются относительно текущего местоположения в дереве. Переходить можно только к узлу конфигурации, который уже создан и зафиксирован. Узлы конфигурации создаются и изменяются с помощью команды `set` и фиксируются с помощью команды `commit`.

Примеры

В приведенном ниже примере работа начинается вверху конфигурации в режиме настройки, далее происходит переход к узлу конфигурации `system login`. По достижении узла `system login` команда `show` отображает в точности содержимое узла `login`. В данном примере обратите внимание на то, как запрос изменяется для отражения местоположения в дереве конфигурации.

Пример 5– Переходы в дереве конфигурации

```
[edit]
admin@edge# edit system login
[edit system login]
admin@edge# show user
   admin {
       authentication {
           encrypted-password $1$EyOd.0dr$j74/m/yLATcXqeiI5zKPR0
           plaintext-password ""
       }
       level admin
   }
   operator1 {
```

```
        authentication {
            encrypted-password $1$Dq/B3sEh$6ng9DikA1nwzGuxuhAyUt1
            plaintext-password ""
        }
        level operator
    }
[edit system login]
admin@edge#
```

5.2.6 exit

Переход на один уровень использования выше:

- от подузла конфигурации – переход к вершине дерева конфигурации;
- от вершины дерева конфигурации – выход в эксплуатационный режим;
- из эксплуатационного режима - выход из системы.

Синтаксис

```
exit [discard]
```

Режим интерфейса

Режим настройки. Эксплуатационный режим.

Ветвь конфигурации

Отсутствует.

Параметры

discard

Применяется при выходе из режима настройки в эксплуатационный режим при незафиксированных изменениях в конфигурации. Позволяет пользователю выйти из режима настройки с отказом ото всех изменений в конфигурации.

Значение по умолчанию

Отсутствует.

Указания по использованию

В результате выполнения данной команды на подузле в дереве конфигурации происходит переход к вершине дерева конфигурации.

В результате выполнения данной команды на вершине дерева конфигурации происходит выход из режима настройки в эксплуатационный режим.

При попытке выхода из режима настройки при наличии незафиксированных изменений в конфигурации система выдаст предупреждение. Выйти из режима настройки будет невозможно до фиксации изменений с помощью команды `commit` или отказа от изменений с помощью команды `exit` с параметром `discard`. Это единственный случай, где применяется параметр.

В результате выполнения данной команды в эксплуатационном режиме происходит выход из системы.

5.2.7 load

Загрузка сохраненной конфигурации.

Синтаксис

```
load [<имя_файла>]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

Отсутствует.

Параметры

имя_файла

Имя файла конфигурации, включая полный путь к его местонахождению.

Указания по использованию

Данная команда используется для загрузки вручную конфигурации, ранее сохраненной в файл.

Загруженная конфигурация становится активной (выполняющейся) конфигурацией, а предыдущая выполняющаяся конфигурация отменяется.

Каталогом конфигурации по умолчанию является `/etc/config`. Так же конфигурацию можно загрузить с жесткого диска по пути, отличающемуся от стандартного каталога `/etc/config`, внешнего накопителя (например, USB-флеш-накопителя), удаленного устройства по протоколам FTP, TFTP, SCP или HTTP.

Если выполняется команда без аргумента, то в качестве загружаемой конфигурации будет использован файл `/etc/config/config.boot`.

В таблице приведен синтаксис способов указания пути для загрузки конфигурационного файла.

Таблица 9 - Способы указания пути для загрузки файла конфигурации

Источник загрузки	**Способ указания**
Локально (абсолютный путь)	Используется стандартный способ указания пути к файлу в UNIX: /путь/имя_файла_конфигурации где путь - путь к расположению файла конфигурации, имя_файла_конфигурации - имя файла конфигурации.
Локально (относительный путь)	Указывается имя файла относительно стандартного каталога конфигурации /etc/config: имя_файла_конфигурации где имя_файла_конфигурации - имя файла конфигурации.
Удаленно (протокол SCP)	Используется следующий синтаксис: scp://имя_пользователя@хост/файл_конфигурации где хост - IP-адрес или имя удаленного хоста с конфигурационным файлом, имя_пользователя - имя пользователя удалённого хоста, файл_конфигурации - имя файла конфигурации, включая путь на удаленном хосте.
Удаленно (протокол FTP)	Используется следующий синтаксис: ftp://имя_пользователя@хост/файл_конфигурации где хост - IP-адрес или имя удаленного хоста с конфигурационным файлом, имя_пользователя - имя пользователя удалённого хоста, файл_конфигурации - имя файла конфигурации, включая путь относительно корневого каталога FTP.
Удаленно (протокол HTTP)	Используется следующий синтаксис: http://хост/файл_конфигурации где хост - IP-адрес или имя удаленного хоста с конфигурационным файлом, файл_конфигурации - имя файла конфигурации, включая путь относительно корневого каталога HTTP.
Удаленно (протокол TFTP)	Используется следующий синтаксис: tftp://хост/файл_конфигурации где хост - IP-адрес или имя удаленного хоста с конфигурационным файлом, файл_конфигурации - имя файла конфигурации, включая путь относительно корневого каталога TFTP.

Обратите внимание, что нельзя загрузить пустой файл конфигурации. В файле конфигурации должен существовать по крайней мере один узел конфигурации. Кроме того, если будет загружен недопустимый файл конфигурации, то будет выдано сообщение об ошибке.

ПРИМЕЧАНИЕ При выполнении загрузки файла конфигурации производится проверка контрольных сумм. В случае несовпадения контрольных сумм на консоль администратору выводится соответствующее предупреждение и просьба подтвердить выполнение дальнейшей загрузки.

Примеры

В примере файл конфигурации `backupconfig` загружается из каталога конфигурации по умолчанию.

Пример 6– Загрузка сохраненной конфигурации из файла

```
[edit]
admin@edge# load backupconfig
Loading configuration from '/etc/config/backupconfig'...
Done
```

Возможные ошибки

При загрузке конфигурации с выключенным управляющим интерфейсом интерфейсу eth0 назначается адрес из подсети 192.168.200.0/24. Пример данной ошибки приведен ниже.

```
admin@edge# load <путь к конфигурационному файлу>
```

При загрузке конфигурации со следующими параметрами:

```
interfaces {
management false
ethernet eth0 {
speed auto
address 192.168.10.1/24
duplex auto
}
}
```

-отключается управляющий интерфейс и задаются адреса для интерфейса eth0. Однако, вместо указанного адреса интерфейсу eth0 назначается адрес из подсети 192.168.200.0/24:

```
[edit]
admin@edge:~$ show interfaces
Interface    IP Address          State       Link    Description
eth0         192.168.200.1/24    up          up
eth1         192.168.11.1/24     up          down
eth2         192.168.12.1/24     up          down
eth3         192.168.13.1/24     up          down
lo           127.0.0.1/8         up          up
lo           ::1/128             up          up
[edit]
admin@edge:~$
```

Для устранения данной ошибки следует выключить управляющий интерфейс:

```
[edit]
admin@edge# set interfaces management false
```

После перезагрузки настроить требуемый адрес.

5.2.8 loadkey

Загрузка пользовательского ключа SSH из файла.

Синтаксис

`loadkey <имя_пользователя> <имя_файла_ключа>`

Режим интерфейса

Режим настройки.

Ветвь конфигурации

Отсутствует.

Параметры

имя_пользователя

Имя пользовательской учетной записи для которой будет добавлен ключ SSH.

имя_файла_ключа

Имя файла, содержащего пользовательский ключ SSH, включая полный путь к его местонахождению.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для загрузки пользовательского ключа SSH из файла для указанной учетной записи.

Загрузить ключ SSH можно из файла, расположенного на жестком диске, внешнем накопителе (например, USB-флеш-накопителе), удаленном устройстве по протоколам FTP, TFTP, SCP или HTTP.

В таблице приведен синтаксис способов указания пути к содержащему пользовательский SSH-ключ файлу.

Таблица 10 - Способы указания пути к содержащему пользовательский SSH-ключ файлу

Источник загрузки	Способ указания
Локально (абсолютный путь)	Используется стандартный способ указания пути к файлу в UNIX: /путь/имя_файла_ключа где путь - путь к расположению файла с ключом SSH, имя_файла_ключа - имя файла, содержащего пользовательский ключ SSH.
Локально (относительный путь)	Указывается имя файла относительно домашнего каталога текущего пользователя: имя_файла_ключа где имя_файла_ключа - имя файла, содержащего пользовательский ключ SSH.
Удаленно (протокол SCP)	Используется следующий синтаксис: scp://имя_пользователя@хост/имя_файла_ключа где хост - IP-адрес или имя удаленного хоста с файлом, содержащим пользовательский ключ SSH, имя_пользователя - имя пользователя удалённого хоста, имя_файла_ключа - имя файла, содержащего пользовательский ключ SSH, включая путь на удаленном хосте.
Удаленно (протокол FTP)	Используется следующий синтаксис: ftp://имя_пользователя @хост/имя_файла_ключа где хост - IP-адрес или имя удаленного хоста с файлом, содержащим пользовательский ключ SSH, имя_пользователя - имя пользователя удалённого хоста, имя_файла_ключа - имя файла, содержащего пользовательский ключ SSH, включая путь относительно корневого каталога FTP.
Удаленно (протокол HTTP)	Используется следующий синтаксис: http://хост/имя_файла_ключа где хост - IP-адрес или имя удаленного хоста с файлом, содержащим пользовательский ключ SSH, имя_файла_ключа - имя файла, содержащего пользовательский ключ SSH, включая путь относительно корневого каталога HTTP.
Удаленно (протокол TFTP)	Используется следующий синтаксис: tftp://хост/имя_файла_ключа где хост - IP-адрес или имя удаленного хоста с файлом, содержащим пользовательский ключ SSH, имя_файла_ключа - имя файла, содержащего пользовательский ключ SSH, включая путь относительно корневого каталога TFTP.

Примеры

В примере осуществляется загрузка пользовательского ключа SSH для пользователя `admin` из файла `pub_key_user`, находящегося на удаленном устройстве, по протоколу SCP. Далее командой `show system login` выводится узел конфигурации с настройками пользователей, где можно увидеть загруженный пользовательский ключ SSH.

Пример 7– Загрузка пользовательского ключа SSH из файла

```
[edit]
admin@edge# loadkey admin scp://user@192.168.10.100/home/user/pub_key_user
user@192.168.10.100's password:
pub_key_user
100%  402     0.4KB/s   00:00
Done
[edit]
admin@edge# show system login
   user admin {
       authentication {
           encrypted-password $1$EyOd.0dr$j74/m/yLATcXqeiI5zKPR0
           plaintext-password ""
           public-keys user@edge {
               key
AAAAB3NzaC1yc2EAAAABJQAAAQEA6CWR1445biyzh18ikIO+LrJmBQ5px0Lgk0svdw/iMbk5KeCUrQ
cfMbnTW1f664Q+J7KSgxqvuRYU/drlYCYKh2+Y0NInd53bsBspDqOJNgjeiVjO0PlPUiKTMW/skRtb
wFwN9kzM4ZvmSgCzPukhVu/WILARQBZn2Cv45XRzfMvlygAQ62OynmxhlI0XAgiccXGH3p9npWQJPw
lpWBy0rg2D2pd2Ht2rRg2Sfd+TK7yurePqvFUgm4gKw6NmAaibR0Ogya4hYMZxdLmayO4C5taYAKxb
GPR7WM+y1z37vczSUdYZz4GvqpeFXJ8i6tQHI1cQCuA6EABB88pSTtvrjw==
               type ssh-rsa
           }
       }
       level admin
   }
```

5.2.9 merge

Слияние сохраненной конфигурации с активной (работающей) конфигурацией.

Синтаксис

```
merge <имя_файла>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

Отсутствует.

Параметры

имя_файла

Имя файла конфигурации, включая полный путь к его местонахождению.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для загрузки вручную конфигурации, ранее сохраненной в файл, и слияния ее с активной (работающей) конфигурацией. В процессе слияния к существующим элементам конфигурации добавляются новые и применяются все изменения, в результате чего получается новая работающая конфигурация, которую можно сохранить.

Каталогом конфигурации по умолчанию является `/etc/config`. Так же конфигурацию можно загрузить с жесткого диска по пути, отличающемуся от стандартного каталога `/etc/config`, внешнего накопителя (например, USB-флеш-накопителя), удаленного устройства по протоколам FTP, TFTP, SCP или HTTP.

Если выполняется команда без аргумента, то в качестве загружаемой конфигурации будет использован файл `/etc/config/config.boot`.

В таблице приведен синтаксис способов указания пути для загрузки конфигурационного файла.

Таблица 11- Способы указания пути для загрузки файла конфигурации

Источник загрузки	**Способ указания**
Локально (абсолютный путь)	Используется стандартный способ указания пути к файлу в UNIX: /путь/имя_файла_конфигурации где путь - путь к расположению файла конфигурации, имя_файла_конфигурации - имя файла конфигурации.
Локально (относительный путь)	Указывается имя файла относительно стандартного каталога конфигурации /etc/config: имя_файла_конфигурации где имя_файла_конфигурации - имя файла конфигурации.
Удаленно (протокол SCP)	Используется следующий синтаксис: scp://имя_пользователя@хост/файл_конфигурации где хост - IP-адрес или имя удаленного хоста с конфигурационным файлом, имя_пользователя - имя пользователя удалённого хоста, файл_конфигурации - имя файла конфигурации, включая путь на удаленном хосте.
Удаленно (протокол FTP)	Используется следующий синтаксис: ftp://имя_пользователя @хост/файл_конфигурации где хост - IP-адрес или имя удаленного хоста с конфигурационным файлом, имя_пользователя - имя пользователя удалённого хоста, файл_конфигурации - имя файла конфигурации, включая путь относительно корневого каталога FTP.
Удаленно (протокол HTTP)	Используется следующий синтаксис: http://хост/файл_конфигурации где хост - IP-адрес или имя удаленного хоста с конфигурационным файлом, файл_конфигурации - имя файла конфигурации, включая путь относительно корневого каталога HTTP.
Удаленно (протокол TFTP)	Используется следующий синтаксис: tftp://хост/файл_конфигурации где хост - IP-адрес или имя удаленного хоста с конфигурационным файлом, файл_конфигурации - имя файла конфигурации, включая путь относительно корневого каталога TFTP.

Примеры

В примере файл конфигурации `backupconfig` загружается из каталога конфигурации по умолчанию и сливается с текущей конфигурацией.

Пример 8– Слияние с конфигурацией, считанной из файла

```
[edit]
admin@edge# merge backupconfig
Loading configuration from '/etc/config/backupconfig'...
Done
```

5.2.10 rename

Изменение идентификатора именованного узла конфигурации.

Синтаксис

```
rename <старое_имя_узла> to <новое_имя_узла>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

Отсутствует.

Параметры

старое_имя_узла

Узел конфигурации, подлежащий переименованию. Формат представляет собой последовательность разделенных пробелами лексем, представляющих имя параметра конфигурации и значение этого параметра; например, `firewall RULE-SET-1`.

новое_имя_узла

Новый идентификатор для узла конфигурации. Формат представляет собой последовательность разделенных пробелами лексем, представляющих имя параметра конфигурации и значение этого параметра; например, `firewall RULE-SET-2`.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для переименования (замены идентификатора) узла конфигурации. Допустимо переименование только тех узлов, которые расположены на текущем редактируемом уровне конфигурации. Текущий уровень конфигурации отображается в квадратных скобках над строкой-приглашением к вводу команд, например, `[edit policy]`.

Для переименования узла конфигурации необходимо с помощью команды `edit` перейти в точку иерархии конфигурации сразу над узлом, который необходимо переименовать. Далее командой `rename` изменить идентификатор.

Если вывести конфигурацию до ее фиксации, можно увидеть, что исходная конфигурация помечена знаком минус ("-"), а новая конфигурация помечена знаком плюс ("+"). Данная пометка и исходный узел конфигурации исчезают после фиксации изменения в конфигурации.

Примеры

В примере выполняется переименование политики межсетевого экранирования `RULE-SET-1` в политику `RULE-SET-2`.

Пример 9– Переименование узла конфигурации

```
[edit]
admin@edge# show policy firewall
   RULE-SET-1 {
        default-action drop
        rule 10 {
            action accept
        }
   }
[edit]
admin@edge# edit policy
[edit policy]
admin@edge# rename firewall RULE-SET-1 to firewall RULE-SET-2
[edit policy]
admin@edge# show
  -firewall RULE-SET-1 {
  -     rule 10 {
  -         action accept
  -     }
  -     default-action drop
  -}
  +firewall RULE-SET-2 {
  +     default-action drop
  +     rule 10 {
  +         action accept
  +     }
  +}
[edit policy]
admin@edge# commit
[edit policy]
admin@edge# show
```

```
   firewall RULE-SET-2 {
       default-action drop
       rule 10 {
           action accept
       }
   }
[edit policy]
admin@edge# top
[edit]
admin@edge#
```

5.2.11 run

Выполнение эксплуатационной команды без выхода из режима настройки.

Синтаксис

```
run <команда>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

Отсутствует.

Параметры

команда

Эксплуатационная команда, которую нужно выполнить.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для выполнения эксплуатационной команды без выхода из режима настройки.

Примеры

В примере из режима настройки выполняется эксплуатационная команда `system date show`.

Пример 10– Выполнение эксплуатационной команды из режима настройки

```
[edit]
admin@edge# run system date show
Пт окт  2 16:05:17 MSK 2020
```

5.2.12 save

Сохранение работающей конфигурации в файл.

Синтаксис

```
save [<имя_файла>]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

Отсутствует.

Параметры

имя_файла

Имя файла конфигурации, включая полный путь к месту его сохранения.

Указания по использованию

Данная команда используется для сохранения выполняющейся конфигурации в файл. Итоговый файл позже может быть загружен в работающую систему с целью замены предыдущей работающей конфигурации при помощи команды `load`.

Каталогом конфигурации по умолчанию является `/etc/config`. Так же конфигурацию можно сохранить на жесткий диск по пути, отличающемуся от стандартного каталога `/etc/config`, внешний накопитель (например, USB-флеш-накопителя), удаленное устройство по протоколам FTP, TFTP, SCP или HTTP. Перед тем, как конфигурацию можно будет сохранить на флэш-накопитель, последний следует проинициализировать командой `flash init` в эксплуатационном режиме.

В таблице приведен синтаксис способов указания пути для сохранения конфигурационного файла.

Таблица 12- Способы указания пути для сохранения файла конфигурации

Место сохранения	**Способ указания**
Локально (абсолютный путь)	Используется стандартный способ указания пути к файлу в UNIX: /путь/имя_файла_конфигурации где путь - путь сохранения файла конфигурации, имя_файла_конфигурации - имя файла конфигурации.
Локально (относительный путь)	Указывается имя файла относительно стандартного каталога конфигурации /etc/config: имя_файла_конфигурации где имя_файла_конфигурации - имя файла конфигурации.
Удаленно (протокол SCP)	Используется следующий синтаксис: scp://имя_пользователя@хост/файл_конфигурации где хост - IP-адрес или имя удаленного хоста для сохранения конфигурационного файла, имя_пользователя - имя пользователя удалённого хоста, файл_конфигурации - имя файла конфигурации, включая путь на удаленном хосте.
Удаленно (протокол FTP)	Используется следующий синтаксис: ftp://имя_пользователя@хост/файл_конфигурации где хост - IP-адрес или имя удаленного хоста для сохранения конфигурационного файла, имя_пользователя - имя пользователя удалённого хоста, файл_конфигурации - имя файла конфигурации, включая путь относительно корневого каталога FTP.
Удаленно (протокол TFTP)	Используется следующий синтаксис: tftp://хост/файл_конфигурации где хост - IP-адрес или имя удаленного хоста для сохранения конфигурационного файла, файл_конфигурации - имя файла конфигурации, включая путь относительно корневого каталога TFTP.

При перезаписи файла конфигурации система создает один файл резервной копии с именем `имя_файла~`. При сохранении перезаписывается файл `config.boot` и система переименовывает предыдущий файл в `config.boot~`.

Обратите внимание, что команда `save` записывает только зафиксированные изменения.

ПРИМЕЧАНИЕ Обратите внимание, при сохранении на локальную систему производится расчет контрольной суммы файла конфигурации. При сохранении файла конфигурации на внешние носители или системы, расчет КС **не производится**.

Примеры

В примере выполняется сохранение работающей конфигурации в файл `config.boot` в каталоге конфигураций по умолчанию, выход из режима настройки и отображение набора файлов, хранящихся в каталоге конфигураций.

Пример 11– Сохранение конфигурации в файл

```
[edit]
admin@edge# save
```

```
Запись конфигурации в '/etc/config/config.boot'...
Готово
[edit]
admin@edge# exit
exit
admin@edge:~$ show files /etc/config
drwxrwxr-x    2 root     root         4.0K Sep 30 04:28 active
-rw-rw----    1 root     vyattacf     3.9K Oct  2 11:06 config.boot
-rw-rw-r--    1 root     vyattacf     3.8K Oct  2 11:06 config.boot~
```

В примере выполняется сохранение текущей работающей конфигурации в файл `backupconfig` в домашнюю директорию пользователя `user` на удаленной рабочей машине, расположенной по адресу 192.168.10.100.

Пример 12– Сохранение конфигурации в файл на удаленной рабочей машине

```
[edit]
admin@edge# save scp://user@192.168.10.100/home/user/backupconfig
Запись конфигурации в 'scp://user@192.168.10.100/home/user/backupconfig'...
user@192.168.10.100's password:
backupconfig
100% 3990     3.9KB/s   00:00
Готово
```

5.2.13 set

Создание нового узла конфигурации или изменение значения в существующем узле конфигурации.

Синтаксис

Синтаксис для создания нового узла конфигурации:

```
set узел [<идентификатор>]
```

Синтаксис для установки атрибута внутри узла конфигурации:

```
set узел [<индентификатор>] <атрибут> [<значение>]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

Отсутствует.

Параметры

узел

Узел конфигурации, который подлежит созданию или изменению, включая полный путь к узлу через конфигурацию в виде последовательности лексем, разделенных пробелами.

идентификатор

Идентификатор узла конфигурации. Обязателен, если узел конфигурации имеет идентификатор; в противном случае недопустим.

атрибут

Атрибут или свойство конфигурации, подлежащий(ее) установке. Если атрибут до этого отсутствует, он создается. Если атрибут уже имеется, его значение заменяется на новое.

значение

Новое значение атрибута. Обязательно, если для атрибута требуется значение; в противном случае недопустимо.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для добавления элемента конфигурации к текущей конфигурации (например, для включения протокола маршрутизации или определения интерфейса). Кроме того, данную команду можно использовать для изменения значения существующего элемента конфигурации. При установке значений в конфигурации обратите внимание на то, что изменение не войдет в силу до тех пор, пока оно не будет зафиксировано при помощи команды `commit`.

После добавления узла конфигурации его можно изменять с помощью команды `set` или удалить с помощью команды `delete`.

Примеры

В примере выполняются добавление узла конфигурации для интерфейса Ethernet и фиксация изменений.

Пример 13– Добавление узла конфигурации

```
[edit]
admin@edge# set interfaces ethernet eth1 address 192.168.10.1/24
[edit]
admin@edge# commit
[edit]
admin@edge# show interfaces ethernet eth1
   address 192.168.10.1/24
```

5.2.14 show

Отображение сведений о конфигурации в режиме настройки.

Синтаксис

`show <узел>`

Режим интерфейса

Режим настройки.

Ветвь конфигурации

Отсутствует.

Параметры

узел

Узел конфигурации, который нужно просмотреть (включая путь).

Значение по умолчанию

При использовании без указания узла конфигурации команда отображает все существующие узлы и подузлы конфигурации начиная с текущего положения в дереве конфигурации.

Указания по использованию

Данная команда используется для отображения настроенного состояния системы в режиме настройки. Команда отображает указанный узел конфигурации и все подузлы. Узлы, находящиеся в процессе удаления или добавления помечаются при просмотре символами "-" или "+" соответственно. Указание узла интерпретируется относительно текущего положения пользователя в дереве конфигурации.

Если параметр `-all` не используется, сведения по умолчанию не включаются в вывод команды.

В дополнение к этой команде есть несколько команд `show` в эксплуатационном режиме.

Примеры

В примере показан узел `service`, отображенный при помощи команды `show` в режиме настройки.

Пример 14– Отображение сведений о конфигурации

```
[edit]
admin@edge# show service
   dhcp-server {
       authoritative disable
       disabled false
       subnet 192.168.10.0/24 {
           lease 86400
           start 192.168.10.1 {
               stop 192.168.10.200
           }
       }
   }
   https {
       x509-cert edge_web_cert
   }
   ssh {
       address 0.0.0.0 {
           port 22
       }
       cipher gost89
       cipher aes128-ctr
       client-alive-timeout 0
       disable-password-authentication false
       hmac hmac-gosthash
       hmac hmac-gosthash2012-256
       hmac hmac-sha1
       key-exchange-algo ecdh-gost2012-512-tc26-paramset-a
       key-exchange-algo diffie-hellman-ec-gost94
       key-exchange-algo diffie-hellman-group-exchange-sha1
   }
[edit]
admin@edge#
```

5.2.15 top

Перемещение на верхний уровень иерархии конфигурации.

Синтаксис

```
top
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

Отсутствует.

Параметры

Отсутствуют.

Указания по использованию

Данная команда используется для быстрого перехода на верхний уровень в режиме настройки.

Примеры

В примере показан переход вниз на несколько узлов дерева конфигурации. Далее использование команды `top` позволяет выполнить переход непосредственно к вершине дерева. В данном примере обратите внимание на то, как в строке `[edit]` отображается текущее положение в дереве конфигурации.

Пример 15– Переход к вершине дерева конфигурации

```
[edit]
```

```
admin@edge# edit interfaces ethernet eth2
[edit interfaces ethernet eth2]
admin@edge# show
   address dhcp
   duplex auto
   mtu 1500
   speed auto
[edit interfaces ethernet eth2]
admin@edge# top
[edit]
admin@edge#
```

5.2.16 up

Перемещение на уровень вверх в дереве конфигурации.

Синтаксис

```
up
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

Отсутствует.

Параметры

Отсутствует.

Указания по использованию

Данная команда используется для перехода на один уровень вверх в режиме настройки.

Примеры

В примере показан переход вниз по нескольким узлам дерева конфигурации, после чего использование команды `up` для последовательного перехода вверх по дереву. В данном примере обратите внимание на то, как в строке `[edit]` отображается текущее положение в дереве конфигурации.

Пример 16– Переход на уровень вверх в дереве конфигурации

```
[edit]
admin@edge# edit interfaces ethernet eth2
[edit interfaces ethernet eth2]
admin@edge# show
   address dhcp
   duplex auto
   mtu 1500
   speed auto
[edit interfaces ethernet eth2]
admin@edge# up
[edit interfaces]
admin@edge# show
   ethernet eth2 {
       address dhcp
       duplex auto
       mtu 1500
       speed auto
   }
   ethernet eth3 {
       address 192.168.13.1/24
   }
   management true
```

```
[edit interfaces]
admin@edge#
```

5.2.17 configure

Вход в режим настройки.

Синтаксис

`configure`

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для входа в режим настройки из эксплуатационного режима. В режиме настройки можно добавлять, удалять и изменять сведения в конфигурации.

В режиме настройки запрос на ввод команд принимает специальный вид, соответствующий режиму.

Примеры

В примере показан отклик системы на вход в режим настройки. В этом примере обратите внимание, что вид запроса на ввод команд изменяется, когда пользователь входит в режим настройки.

Пример 17– Вход в режим настройки

```
admin@edge:~$ configure
[edit]
admin@edge#
```

5.2.18 show configuration

Отображение конфигурации системы из эксплуатационного режима.

Синтаксис

`show configuration [all | cmds | files]`

Режим интерфейса

Эксплуатационный режим.

Параметры

all

Отображение всей конфигурации, в том числе обычно не отображаемых значений по умолчанию.

cmds

Отображение конфигурации в формате команд режима настройки. Отображается ранее сохраненная конфигурация (при помощи команды `save`).

files

Отображение списка файлов конфигурации в `/etc/config`.

Значение по умолчанию

Отображаются только явно установленные значения (то есть значения не по умолчанию).

Указания по использованию

Данная команда используется для вывода сведений о конфигурации без выхода из эксплуатационного режима. Использование команды `show configuration` в эксплуатационном режиме эквивалентно использованию команды `show` в режиме настройки.

Примеры

В примере показано отображение конфигурации из эксплуатационного режима. (Для краткости показан только первый экран сведений).

Пример 18– Отображение сведений о конфигурации в эксплуатационном режиме

```
admin@edge:~$ show configuration
  pki {
      ca defaultca {
          certificate edge_web_cert {
              key-type gost2001
              cn "Numa Edge Web Interface"
              email root@numa-edge
              expires-on "Sun Feb 23 17:30:13 2025"
          }
          cn "Default Numa Edge CA"
          expires-on "Mon Feb 24 17:30:13 2025"
          key-type gost2001
      }
  }
  system {
      host-name edge
      time-zone Europe/Moscow
      login {
          user admin {
              authentication {
                  encrypted-password ****************
                  plaintext-password ****************
              }
              level admin
          }
...
```

6 Настройка даты и времени

В разделе приведена информация по использованию функции настройки даты и времени в системе Numa Edge, примеры настроек и описание команд, используемых при работе с данной функцией.

- Обзор функции настройки даты и времени
- Примеры настройки
- Команды управления

6.1 Обзор функции настройки даты и времени

Numa Edge позволяет производить настройку даты и времени как вручную, с помощью команды `system date set <дата_и_время>`, так и осуществляя синхронизацию системы с одним или несколькими серверами протокола NTP (сетевого времени), с помощью команды `system date set ntp <сервер_ntp>`.

Установка часового пояса осуществляется вручную либо как разница с гринвичским временем (UTC), либо как номер поддерживаемого буквального часового пояса. Для определения часового пояса используется команда `system time-zone <временная_зона>`.

Numa Edge может быть настроен как в режиме клиента (используя удаленные сервера NTP) или в режиме сервера (являясь непосредственно сервером NTP), так и в обоих режимах одновременно.

При работе в режиме клиента, для автоматической синхронизации времени с удаленным NTP-сервером используется команда `system ntp server <сервер_ntp>` с указанием IP-адреса, либо имени NTP сервера. Если в качестве удаленного NTP сервера указывается пул серверов, то синхронизация будет производиться только с одним сервером из пула. Для разрешения осуществления скачковой синхронизации времени (т.е. для моментальной синхронизации времени системы с серверами NTP) используется команда `system ntp step-at-start <состояние>`.

При работе в режиме сервера, для указания IP-адреса сетевого интерфейса, на котором будут прослушиваться NTP-запросы, используется команда `service ntp listen-on <адрес>`. Для указания страты сервера используется команда `service ntp stratum <уровень>`. Следует отметить, что указывать страту сервера необходимо при работе исключительно в режиме сервера. При работе одновременно как в режиме сервера, так и в режиме клиента, страта локального сервера назначается автоматически, однако предусматривается возможность принудительного указания страты.

6.2 Примеры настройки

В этом разделе представлены эталонные настройки для сопровождения сведений о дате и времени. В частности, рассматриваются следующие вопросы:

- Установка даты и времени вручную
- Синхронизация с сервером NTP вручную
- Настройка часового пояса
- Настройка автоматической синхронизации с NTP серверами в режиме клиента
- Скачковая синхронизация времени режиме клиента
- Настройка локального NTP сервера на сетевом интерфейсе
- Указание страты в режиме сервера

Используемая настройка маршрутизатора R1 показана на рисунке ниже

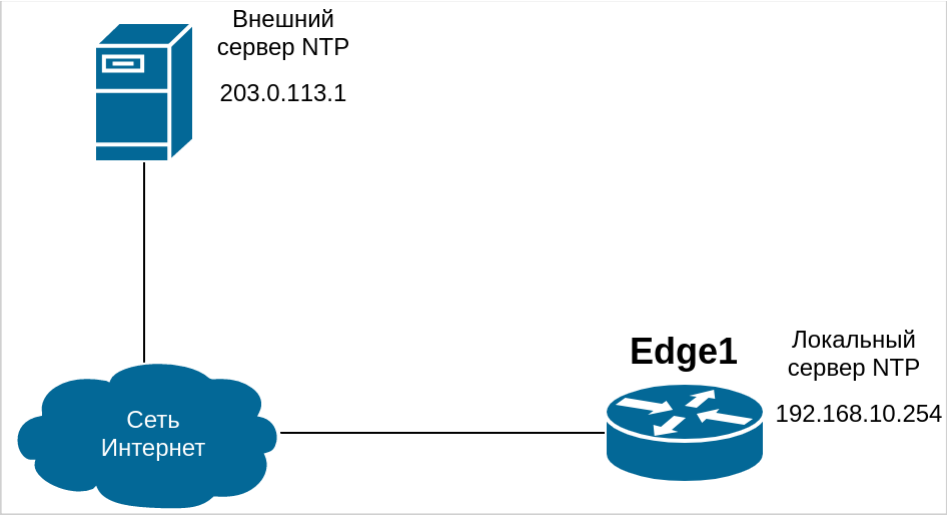


Рисунок 3 – Установка даты и времени

6.2.1 Установка даты и времени вручную

В примере выполняется установка даты вручную на 13:15 ровно 24 апреля 2018 г. Используется формат `ГГГГ.ММ.ДД-чч:мм`. Возможны также форматы `ММ.ДД-чч:мм`, `ГГГГ.ММ.ДД-чч:мм:сс` и `ММ.ДД-чч:мм:сс`.

Для установки даты вручную необходимо выполнить следующие действия в эксплуатационном режиме:

Пример 19– Установка даты и времени вручную

Действие	**Команда**
Указание даты. Используется формат ГГГГ.ММ.ДД-01:мм	`admin@Edge1:~$ system date set 2018.04.24-13:15`
Проверка применения настроек даты и времени	`admin@Edge1:~$ date` `Вт апр 24 13:15:03 MSK 2018`

6.2.2 Синхронизация с сервером NTP вручную

В примере вручную выполняется синхронизация часов системы с сервером NTP по адресу 203.0.113.42.

Следует обратить внимание, что это всего лишь выполнение одноразовой синхронизации. Постоянное соединение с сервером NTP при этом не устанавливается. Сведения об установке автоматической синхронизации приведены в разделе «Настройка автоматической синхронизации с NTP серверами в режиме клиента».

Для выполнения одноразовой синхронизации с сервером NTP необходимо выполнить следующие действия в эксплуатационном режиме:

Пример 20– Синхронизация системы с сервером NTP вручную

Действие	**Команда**

Синхронизация с удаленным NTP сервером	`admin@Edge1:~$ system date set ntp 203.0.113.42`
	`Синхронизация с NTP сервером … завершена`
	`set local clock to Tue Apr 24 13:15:20 MSK 2018`
	`admin@Edge1:~$`

6.2.3 Настройка часового пояса

Часовой пояс настраивается при помощи команды `system time-zone`. Для этого нужно указать регион/местоположение, которые наилучшим образом соответствуют местоположению межсетевого экрана. Например, если указать **Asia/Vladivostok**, будет установлен часовой пояс, соответствующий городу Владивосток (Россия). Для вывода доступных часовых поясов можно использовать автозавершение команд (т.е. клавишу <Tab>). Переключение на летнее время и назад будет происходить автоматически в зависимости от времени года и выбранного региона.

В примере выполняется установка часового пояса, соответствующего городу Владивосток (Россия). Для установки часового пояса необходимо выполнить следующие действия в режиме настройки:

Пример 21– Установка часового пояса

Действие	Команда
Установка часового пояса	[edit] admin@Edge1# set system time-zone Asia/Vladivostok
Фиксация сведений	[edit] admin@Edge1# commit
Отображение настройки	[edit] admin@Edge1# show system time-zone time-zone Asia/Vladivostok

6.2.4 Настройка автоматической синхронизации с NTP серверами в режиме клиента

В режиме клиента, автоматическая синхронизация осуществляется путем настройки соединения с сервером NTP при помощи команды `system ntp server` с указанием IP-адреса, либо имени NTP сервера.

В примере выполняется настройка автоматической синхронизации с двумя серверами NTP по следующим адресам:

- 203.0.113.1;
- ntp.example.org.

Для указания серверов NTP необходимо выполнить следующие действия в режиме настройки:

Пример 22– Установка автоматической синхронизации с NTP серверами

Действие	Команда
Указание NTP сервера по адресу 203.0.113.42	[edit] admin@Edge1# set system ntp server 203.0.113.1
Указание NTP сервера с именем ntp.example.org	[edit] admin@Edge1# set system ntp server ntp.example.org
Фиксация сведений	[edit] admin@Edge1# commit
Отображение настройки	[edit] admin@Edge1# show system ntp server server 203.0.113.1 server ntp.example.org

В примере выполняется настройка автоматической синхронизации с сервером и настройка часового пояса для устройства, находящегося в Москве.

Пример 23– Настройка автоматической синхронизации с сервером и настройка часового пояса для устройства, находящегося в Москве

Действие	Команда
Установка часового пояса для Москвы	[edit] admin@Edge1# set system time-zone Europe/Moscow
Указание NTP сервера с именем ntp1.stratum2.ru	[edit] admin@Edge1# set system ntp server ntp1.stratum2.ru
Фиксация сведений	[edit] admin@Edge1# commit
Отображение настройки	[edit] admin@Edge1# show system ntp server server ntp1.stratum2.ru [edit] admin@Edge1# show system time-zone time-zone Europe/Moscow

6.2.5 Скачковая синхронизация времени режиме клиента

В примере выполняется разрешение скачковой синхронизации с использованием команды `system ntp step-at-start`. При указании состояния используются значения **true** (разрешено) или **false** (запрещено; значение по умолчанию).

Для разрешения скачковой синхронизации времени необходимо выполнить следующие действия в режиме настройки:

Пример 24– Скачковая синхронизация времени при запуске сервера NTP

Действие	**Команда**
Разрешение скачковой синхронизации времени	`[edit]` `admin@Edge1# set system ntp step-at-start true`
Фиксация сведений	`[edit]` `admin@Edge1# commit`

Отображение настройки	`[edit]`
	`admin@Edge1# show system ntp step-at-start`
	`step-at-start true`

6.2.6 Настройка локального NTP сервера на сетевом интерфейсе

В примере с помощью команды `service ntp listen-on` указывается IP-адрес сетевого интерфейса, на котором будет проводиться прослушка NTP-запросов.

Для прослушки NTP-запросов, необходимо выполнить следующие действия в режиме конфигурации:

Пример 25– Прослушка NTP-запросов

Действие	**Команда**
Указание IP-адреса сетевого интерфейса, на котором будет проводиться прослушка NTP-запросов	`[edit]` `admin@Edge1# set service ntp listen-on 192.168.10.254`
Фиксация сведений	`[edit]` `admin@Edge1# commit`

Отображение настройки	`[edit]`
	`admin@Edge1# show service ntp listen-on`
	`listen-on 192.168.10.254`

6.2.7 Указание страты в режиме сервера

При работе в режиме сервера NTP, указание страты необходимо для определения его уровня в иерархической системе источников времени.

В примере выполняется указание страты сервера NTP при помощи команды `service ntp stratum`.

Для указания страты сервера NTP необходимо выполнить следующие действия в режиме настройки:

Пример 26– Указание страты для сервера NTP

Действие	**Команда**
Указание страты сервера NTP	`[edit]` `admin@Edge1# set service ntp stratum 1`
Фиксация сведений	`[edit]` `admin@Edge1# commit`

Отображение настройки	`[edit]`
	`admin@Edge1# show service ntp stratum`
	`stratum 1`

6.3 Команды управления

Команды настройки	
system time-zone <временная зона>	Установка часового пояса как региона/местоположения
system ntp server <сервер_ntp>	Установка автоматической синхронизации с NTP сервером при работе в режиме клиента
system ntp step-at-start <состояние>	Скачковая синхронизация времени при работе режиме в клиента
service ntp active <состояние>	Возможность отключения сервиса NTP с сохранением настройки
service ntp listen-on <адрес>	Указание IP-адреса сетевого интерфейса, на котором будут прослушиваться запросы NTP при работе в режиме сервера
service ntp stratum <уровень>	Указание страты при работе в режиме сервера
Эксплуатационные команды	
system date show	Установка даты и времени системы непосредственно или указание сервера NTP, с которого их следует принять.
system date set	Отображение даты и времени системы.
show ntp	Отображение состояния настроенных серверов NTP.

6.3.1 system time-zone <временная зона>

Установка часового пояса как региона/местоположения.

Синтаксис

```
set system time-zone <временная_зона>
delete system time-zone
show system time-zone
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   time-zone временная_зона
}
```

Параметры

временная_зона

Строка, обозначающая временную зону. Ее формат регион/местоположение.

Значение по умолчанию

Значение по умолчанию Europe/Moscow.

Указания по использованию

Эта команда используется для установки часового пояса для локальных часов системы. Для этого следует указать регион и местоположение в формате регион/местоположение. Следует заметить, что регион и местоположение зависят от регистра символов. Для отображения различных вариантов следует использовать автозавершение команд (т.е. клавишу <Tab>).

В дополнение к широкому кругу доступных пар регион/местоположение, поддерживается обратная совместимость при помощи формата `Etc/<сдвиг>` вместо регион/местоположение. Обратите внимание, что в записи `Etc/<сдвиг>` используется сдвиг в формате Posix. Это значит, что положительный сдвиг используется для указания региона к западу от Гринвича, а не к востоку от Гринвича, как во многих системах. Например, `Etc/GMT+8` соответствует 8 часам позади UTC (то есть к западу от Гринвича).

Форма **set** этой команды используется для установки временной зоны системы.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** этой команды может использоваться для просмотра установленного часового пояса.

6.3.2 system ntp server <сервер_ntp>

Установка автоматической синхронизации с NTP серверами при работе в режиме клиента.

Синтаксис

```
set system ntp server <сервер_ntp>
delete system ntp server <сервер_ntp>
show system ntp server
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   ntp {
      server сервер_ntp
   }
}
```

Параметры

сервер_ntp

Множественный узел. IPv4-адрес или имя узла сервера NTP. Система автоматически получит дату и время системы с указанного сервера.

Можно указать несколько серверов NTP, создав несколько экземпляров узла конфигурации **server**.

Значение по умолчанию

Отсутствует.

ПРИМЕЧАНИЕ Если в качестве имени сервера указывается имя пула, разрешающееся в несколько адресов, то синхронизация будет проводиться по всем доступным адресам.

Указания по использованию

Эта команда используется для указания серверов NTP для данной системы.

Форма **set** этой команды используется для указания сервера NTP для синхронизации времени.

Форма **delete** этой команды используется для отмены автоматической синхронизации с указанным сервером NTP.

Форма **show** этой команды может использоваться для просмотра списка определенных серверов NTP.

6.3.3 system ntp step-at-start <состояние>

Разрешение скачковой синхронизация времени при работе режиме в клиента.

Синтаксис

```
set system ntp step-at-start <состояние>
delete system ntp step-at-start
show system ntp step-at-start
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
```

```
    ntp {
        step-at-start состояние
    }
}
```

Параметры

состояние

Допустимые значения:

true: скачковая синхронизация времени разрешена.

false: скачковая синхронизация времени запрещена.

Значение по умолчанию

По умолчанию, используется значение `false`.

Указания по использованию

Эта команда используется для разрешения скачковой синхронизации времени. По умолчанию, в случае если разница во времени с сервером NTP, с которым производится синхронизация, превышает `1000s`, синхронизация времени завершается сообщением об ошибке. Установка параметра **step-at-start** в значение **true** позволяет проводить синхронизацию с сервером NTP независимо от разницы во времени.

Форма **set** этой команды устанавливает режим работы скачковой синхронизации времени.

Форма **delete** этой команды устанавливает режим скачковой синхронизации по умолчанию.

Форма **show** этой команды может использоваться для просмотра текущей настройки режима скачковой синхронизации времени.

6.3.4 service ntp active <состояние>

Возможность отключения сервиса NTP с сохранением настройки.

Синтаксис

```
set service ntp active <состояние>
delete service ntp active
show service ntp active
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    ntp {
      active <состояние>
    }
}
```

Параметры

состояние

Административное состояние сервиса NTP. Поддерживаются следующие значения:

on: Включение сервиса NTP.

off: Отключение сервиса NTP без отбрасывания настройки.

Значение по умолчанию

Сервис NTP включен.

Указания по использованию

Эта команда используется для отключения сервиса NTP с сохранением настройки.

Форма **set** данной команды используется для указания состояния сервиса NTP.

Форма **delete** этой команды используется для восстановления состояния по умолчанию.

Форма **show** этой команды может использоваться для просмотра состояния сервиса NTP.

6.3.5 service ntp listen-on <адрес>

Указание IP-адреса сетевого интерфейса, на котором будут прослушиваться запросы NTP при работе в режиме сервера.

Синтаксис

```
set service ntp listen-on <адрес>
delete service ntp listen-on <адрес>
show service ntp listen-on
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   ntp {
     listen-on <адрес>
   }
}
```

Параметры

адрес

Обязательный параметр. Множественный узел. Адрес сетевого интерфейса, на котором следует прослушивать запросы NTP. Поддерживаются как адреса IPv4, так и IPv6.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания IP-адреса сетевого интерфейса, на которых следует прослушивать запросы NTP.

Форма **set** данной команды устанавливает адрес интерфейса для прослушивания запросов NTP.

Форма **delete** этой команды удаляет указанную настройку.

Форма **show** этой команды может использоваться для просмотра настройки прослушивания NTP-запросов.

6.3.6 service ntp stratum <уровень>

Указание страты при работе в режиме сервера.

Синтаксис

```
set service ntp stratum <уровень>
delete service ntp stratum
show service ntp stratum
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
```

```
    ntp {
        stratum уровень
    }
}
```

Параметры

уровень

Числовой идентификатор. Значение в диапазоне от 1 до 16. При указании уровня равным 16, клиенты будут рассматривать локальный сервер как некорректный.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания страты сервера NTP.

Форма **set** этой команды используется для указания страты сервера NTP.

Форма **delete** этой команды используется для удаления параметра.

Форма **show** этой команды может использоваться для просмотра текущего значения страты сервера NTP.

6.3.7 system date set

Установка даты и времени системы непосредственно или указание сервера NTP, с которого их следует принять.

Синтаксис

```
system date set [<utc> <дата_и_время> | <дата_и_время> | ntp <сервер_ntp>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

дата_и_время

Установка даты и времени непосредственно в одном из следующих форматов:

- ГГГГ.ММ.ДД-чч:мм:сс
- ГГГГ.ММ.ДД-чч:мм
- ММ.ДД-чч:мм:сс
- ММ.ДД-чч:мм

Обратите внимание, что в поле часов (чч) используется 24-часовая запись (например, 3:00 пополудни будет представлено числом 15 в поле часов). При использовании параметра utc время задается в UTC.

сервер_ntp

Указание сервера протокола NTP, с которого следует принять время. Для определения сервера NTP можно указать либо IPv4-адрес, либо имя узла.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки даты и времени системы либо непосредственно, либо путем указания сервера NTP, с которого следует принять дату и время. Если часовой пояс не настроен, предполагается всемирное координированное время. Часовой пояс устанавливается с помощью команды `system time-zone <часовой_пояс>`.

При синхронизации времени с сервером NTP может потребоваться предварительно включить режим скачковой синхронизации командой `system ntp step-at-start <состояние>`.

Примеры

В примере выполняется установка даты и времени системы на 10:55 15 мая 2018 г.

Пример 27– Установка даты и времени в UTC непосредственно

```
admin@edge:~$ system date set utc 2018.05.25-15:55
admin@edge:~$
```

В примере выполняется установка даты и времени системы с использованием сервера NTP.

Пример 28– Установка даты и времени при помощи сервера NTP

```
admin@edge:~$ system date set ntp 0.pool.ntp.org
Синхронизация с NTP сервером ... завершена
set local clock to Tue Oct 30 19:51:21 MSK 2018 (offset 14493292.537571s)
admin@edge:~$
```

6.3.8 system date show

Отображение даты и времени системы.

Синтаксис

```
system date show [utc]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

utc

Отображение даты и времени в координированном всемирном времени.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения даты и времени системы либо в локальном времени, либо в UTC.

Примеры

В примере показаны дата и время системы edge.

Пример 29– Отображение даты и времени системы

```
admin@edge:~$ system date show
Tue Oct 30 16:55:07 MSK 2018
admin@edge:~$
```

6.3.9 show ntp

Отображение состояния настроенных серверов NTP.

Синтаксис

```
show ntp [<имя> | <ipv4-адрес> | 0.ru.pool.ntp.org]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя

Вывод состояния подключения к серверу NTP с указанным именем узла.

ipv4-адрес

Вывод состояния подключения к серверу NTP с указанным IPv4-адресом.

0.ru.pool.ntp.org

Вывод состояния подключения к серверу NTP по умолчанию.

Значение по умолчанию

При выполнении команды без параметров выводятся сведения обо всех серверах NTP, указанных в узле **system ntp server** конфигурационного режима.

Указания по использованию

Эта команда используется для просмотра состояния подключений к настроенным серверам NTP.

Для каждого настроенного сервера NTP выдается строчка, в которой выводятся IP-адрес сервера и его параметры.

Подключения к серверам NTP настраиваются при помощи команды `system ntp server <имя>`.

Примеры

В примере выводится команда show ntp.

Пример 30– Вывод настроенных серверов NTP

```
admin@edge:~$ show ntp
4/4 peers valid, clock unsynced, clock offset is 574.058ms

peer
   wt tl st  next  poll          offset       delay      jitter
188.93.104.2 from pool 0.ru.pool.ntp.org
    1 10  2   21s   33s         0.866ms    13.111ms     1.806ms
88.212.196.95 from pool 0.ru.pool.ntp.org
    1 10  3   18s   32s        -1.262ms    11.466ms     0.647ms
46.17.104.93 from pool 0.ru.pool.ntp.org
    1 10  2   24s   34s        -0.385ms    13.726ms     2.984ms
85.21.78.23 from pool 0.ru.pool.ntp.org
    1 10  2   26s   33s        -0.086ms    10.971ms     0.357ms
admin@edge:~$
```

7 Управление системой

В этом разделе описаны функции системы Numa Edge для основных задач управления системой, таких как установка сведений об узле, работа с кэшем ARP и установка системных даты и времени.

В этом разделе рассматриваются следующие вопросы:

- Основная настройка системы
- Наблюдение за сведениями о системе
- Команды управления системой

7.1 Основная настройка системы

Команды, описанные в этом разделе, позволяют изменить и просмотреть основные сведения о системе. В этом разделе рассматриваются следующие вопросы:

- Настройка сведений об узле
- Настройка DNS

7.1.1 Настройка сведений об узле

В этом разделе рассматриваются следующие вопросы:

- Установка имени узла системы
- Установка домена системы
- IP-адрес системы
- Шлюз по умолчанию
- Псевдонимы

В этом разделе представлены эталонные настройки для сведений об узле системы. Используемая эталонная настройка показана на рисунке.

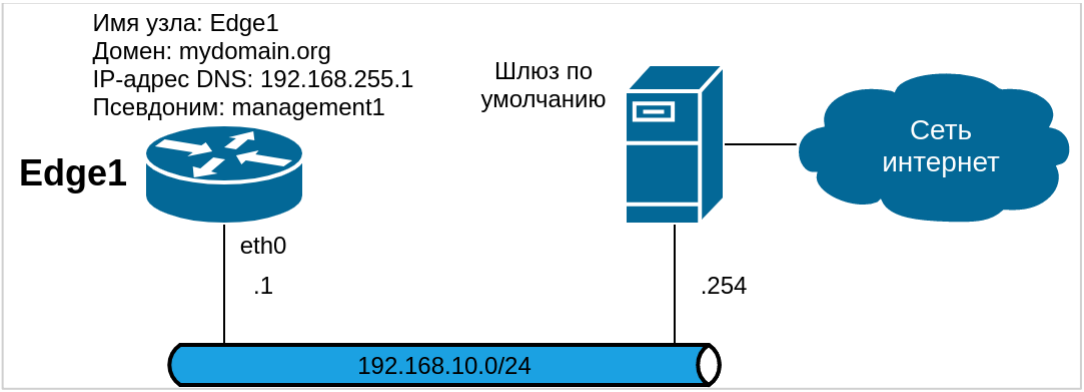


Рисунок 4 – Сведения об узле

Установка имени узла системы

Имя системы Numa Edge устанавливается с помощью команды `system host-name`. В имя системы могут входить буквы, цифры и дефисы ("-").

В примере показана установка имени узла системы в Edge1. Для установки имени узла системы нужно выполнить следующие действия в режиме настройки:

Пример 31– Установка имени узла системы

Действие	**Команда**
Установка имени узла системы	`[edit]` `admin@edge# set system host-name Edge1`
Фиксация изменения	`[edit]`

	admin@edge# commit
Вид запроса на ввод команд изменяется, отражая изменение (соответствующие изменения произойдут после повторного входа в систему)	[edit] admin@Edge1#
Отображение настройки	[edit] admin@Edge1# show system host-name host-name Edge1

Установка домена системы

Домен системы устанавливается при помощи команды `system dns domain-name`. В имена доменов могут входить буквы, цифры, дефисы и точки.

ПРИМЕЧАНИЕ Команды `system dns domain-name` и `system dns domain-search` являются взаимоисключающими. Одновременно может быть настроена только одна из них.

В примере домен системы устанавливается на `mydomain.com`. Для установки домена системы нужно выполнить следующие действия в режиме настройки:

Пример 32– Установка домена системы

Действие	Команда
Установка имени домена	[edit] admin@Edge1# set system dns domain-name mydomain.org
Фиксация изменения	[edit] admin@Edge1# commit
Отображение настройки	[edit] admin@Edge1# show system dns domain-name domain-name mydomain.org

IP-адрес системы

IP-адрес системы можно статически сопоставить с именем узла для нужд локальной службы DNS при помощи команды `system static-host-mapping`.

Сети IP указываются в формате CIDR — то есть в записи ip-адрес/префикс, например 192.168.12.0/24. Для единичных адресов используется четверка чисел, разделенных точками: a.b.c.d. В качестве сетевого префикса вводится десятичное число от 1 до 32 включительно.

Хорошая практическая рекомендация - сопоставить имя узла системы с адресом интерфейса-заглушки (loopback), так как последний является наиболее надежным интерфейсом в системе. В данном примере интерфейсу-заглушке дан адрес 192.168.255.1. Это адрес, настроенный для интерфейса-заглушки в эталонной топологии, используемой в данном руководстве.

В примере создается статическое сопоставление между именем узла Edge1 и IP-адресом 192.168.255.1. Это IP-адрес, который сервер DNS будет использовать для разрешения запросов DNS к Edge1.mydomain.org.

Для сопоставления имени узла и IP-адреса нужно выполнить следующие действия в режиме настройки:

Пример 33– Сопоставление IP-адреса системы с ее именем узла

Действие	Команда
Сопоставление имени узла Edge1 с IP-адресом	[edit] admin@Edge1# set system static-host-mapping host-name Edge1 inet 192.168.255.1
Фиксация изменения	[edit] admin@Edge1# commit

Отображение настройки	[edit]
	admin@Edge1# show system static-host-mapping
	host-name Edge1 {
	inet 192.168.255.1
	}

Шлюз по умолчанию

В примере в качестве шлюза по умолчанию для системы указывается 192.168.10.254. Для указания шлюза по умолчанию нужно выполнить следующие действия в режиме настройки:

Пример 34– Установка шлюза по умолчанию

Действие	Команда
Указание шлюза по умолчанию	`[edit]` `admin@Edge1# set system gateway-address 192.168.10.254`
Фиксация изменения	`[edit]` `admin@Edge1# commit`

Отображение настройки	`[edit]`
	`admin@Edge1# show system gateway-address`
	`gateway-address 192.168.10.254`

Псевдонимы

Для системы можно определить один или несколько псевдонимов путем сопоставления IP-адреса системы с более чем одним именем узла. В примере выполняется создание псевдонима `management1` для системы. Для создания псевдонима для системы нужно выполнить следующие действия в режиме настройки:

Пример 35– Создание псевдонима для системы

Действие	Команда
Определение псевдонима	`[edit]` `admin@Edge1# set system static-host-mapping host-name Edge1 alias management1`
Фиксация изменения	`[edit]` `admin@Edge1# commit`

Отображение настройки	`[edit]`
	`admin@Edge1# show system static-host-mapping`
	`host-name Edge1 {`
	`alias management1`
	`inet 192.168.255.1`
	`}`

7.1.2 Настройка DNS

В этом разделе рассматриваются следующие вопросы:

- Серверы имен DNS
- Порядок поиска домена

В этом разделе представлены эталонные настройки для сведений о DNS. Использованная настройка DNS показана на рисунке.

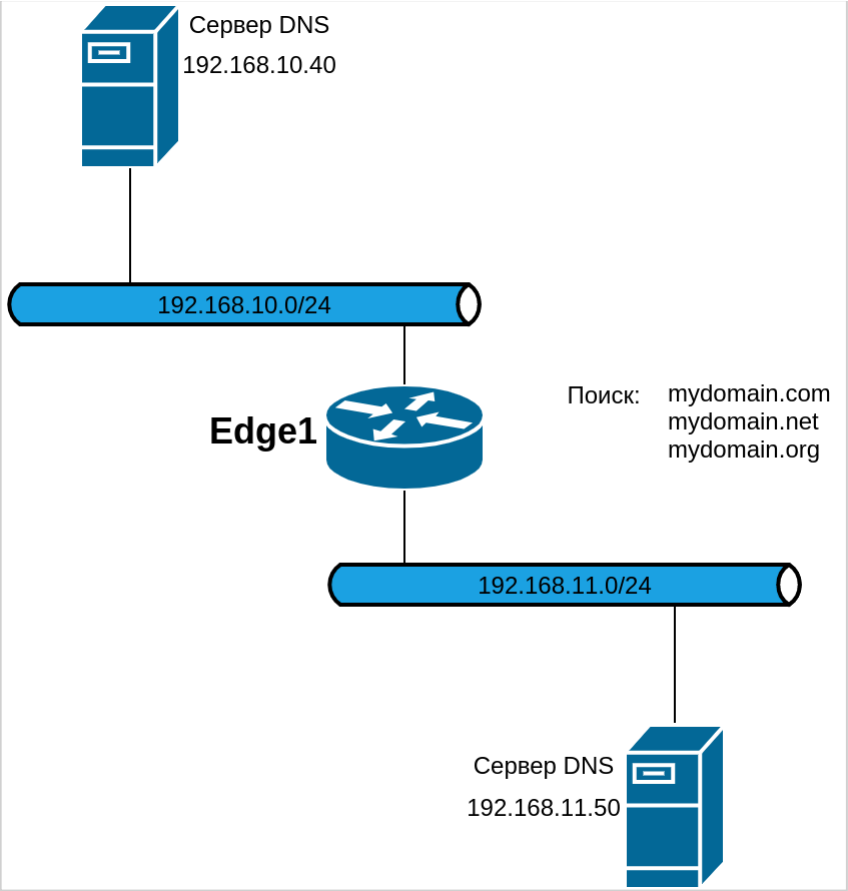


Рисунок 5 – Настройка DNS

Серверы имен DNS

Серверы имен DNS указываются при помощи команды `system dns name-server`.

В примере указывается два сервера DNS для системы: один с адресом 192.168.10.40, другой с адресом 192.168.11.50.

Для указания серверов DNS нужно выполнить следующие действия в режиме настройки:

Пример 36– Указание серверов имен DNS

Действие	**Команда**
Указание первого сервера DNS	`[edit]` `admin@Edge1# set system  dns name-server 192.168.10.40`
Указание второго сервера DNS.	`[edit]` `admin@Edge1# set system dns name-server 192.168.11.50`
Фиксация изменения.	`[edit]` `admin@Edge1# commit`

Отображение настройки.	`[edit]`
	`admin@Edge1# show system  dns name-server`
	`  name-server 10.10.40.34 {`
	`  }`
	`  name-server 192.168.11.50 {`
	`  }`

Порядок поиска домена

Для системы можно указать список доменов, которые можно использовать для завершения недоопределенного имени узла. Для определения этого списка нужно указать порядок поиска среди этих доменов с помощью команды `system dns domain-search`.

ПРИМЕЧАНИЕ Команды **system dns domain-name** и **system dns domain-search** являются взаимоисключающими. Одновременно может быть настроена только одна из них.

Для команды `system dns domain-search` требуется ввод каждого имени домена по отдельности в порядке, в котором нужно в дальнейшем производить поиск. В имя домена могут входить буквы, цифры, дефисы ("-") и точки (".").

В примере системе дается указание пытаться завершать доменные имена в следующем порядке: первым mydomain.com, вторым mydomain.net, последним mydomain.org.

Для указания порядка поиска домена нужно выполнить следующие действия в режиме настройки:

Пример 37– Установка порядка поиска для автозавершения домена

Действие	**Команда**
Указание первого имени домена.	`[edit]` `admin@Edge1# set system dns domain-search domain mydomain.com`
Указание второго имени домена.	`[edit]` `admin@Edge1# set system dns domain-search domain mydomain.net`
Указание третьего имени домена.	`[edit]` `admin@Edge1# set system dns domain-search domain mydomain.org`
Фиксация изменения.	`[edit]` `admin@Edge1# commit`

Отображение настройки.	`[edit]`
	`admin@Edge1# show system dns domain-search`
	`domain mydomain.com`
	`domain mydomain.net`
	`domain mydomain.org`

7.2 Наблюдение за сведениями о системе

7.2.1 Отображение сведений об узле

Для просмотра настроенного имени узла используется команда `show host name` в эксплуатационном режиме, как показано в примере:

Пример 38– Отображение имени узла системы

```
admin@Edge1:~$ show host name
Edge1
admin@Edge1:~$
```

7.2.2 Отображение даты и времени

Для просмотра времени в соответствии с системными часами используется команда show host date в эксплуатационном режиме, как показано в примере:

Пример 39– Отображение даты и времени системы

```
admin@Edge1:~$ system date show
Вт окт 30 16:01:17 MSK 2018
admin@Edge1:~$
```

7.3 Команды управления системой

Команды управления системой

Команды настройки	
system country <код страны>	Указание двухзначного кода страны.

Команды настройки	
system dns domain-name <домен>	Установка домена системы.
system dns domain-search domain <домен>	Определение набора доменов для автозавершения домена.
system dns name-server <адрес>	Указание серверов имен DNS, доступных системе.
system dns cache-size <размер>	Указание размера кэша службы ретрансляции DNS
system dns dnssec check-unsigned <состояние>	Проверка доменной зоны для неподписанного DNS-ответа
system dns dnssec disable	Отключение поддержки DNSSEC
system dns dnssec trust-anchor <имя>	Указание имени якоря доверия
system dns dnssec trust-anchor <имя> algorithm <алгоритм>	Указание алгоритма подписи
system dns dnssec trust-anchor <имя> digest-type <алгоритм_хеширования>	Указание алгоритма хеширования
system dns dnssec trust-anchor <имя> digest <хеш>	Указание хеша
system dns dnssec trust-anchor <имя> domain <домен>	Указание имени домена
system dns dnssec trust-anchor <имя> key-tag <маркер_ключа>	Указание маркера ключа
system gateway-address <адрес>	Указание шлюза по умолчанию для системы.
system host-name <имя>	Установка имени узла для системы (по умолчанию: edge) .
system options reboot-on-panic <режим>	Установка поведения системы при неисправимой ошибке.
system static-host-mapping host-name <имя>	Определение статического сопоставления между именем узла и IP-адресом.
system static-host-mapping local-ttl <время_жизни>	Установка периода времени, в течение которого клиент будет считать полученную информацию о сопоставлении актуальной.
system time-zone <часовой_пояс>	Установка часового пояса для локальных системных часов.
system watchdog	Настройки сторожевого таймера
system ip arp table-size <размер>	Указание максимального количества записей, которые хранятся в кэше ARP.
system ip disable-forwarding	Установка запрета на перенаправление IPv4-пакетов на всех интерфейсах.
system ipv6 disable	Установка запрета на присвоение IPv6-адресов для всех интерфейсов.
system ipv6 disable-forwarding	Запрет перенаправления IPv6-пакетов на всех интерфейсах.
system ipv6 neighbor table-size <размер>	Указание максимального количества записей, которые хранятся в таблице соседей IPv6.
system ipv6 strict-dad	Включение блокировки IPv6-протокола на интерфейсе после обнаружения дублирующего link-local адреса (MAC адреса интерфейса Ethernet) с помощью протокола определения дублирующего адреса (Duplicate Address Detection – DAD).
system ssh cipher <алгоритм>	Указание допустимых для использования клиентом SSH алгоритмов шифрования.
system ssh hmac <алгоритм>	Указание допустимых алгоритмов выработки имитовставки для клиента SSH.
system ssh key-exchange-algo <алгоритм>	Указание допустимых алгоритмов обмена ключами для клиента SSH.
system ssh hostkey-algo <алгоритм>	Указание допустимых алгоритмов асимметричного шифрования для клиента SSH.
Настройка параметров подключения к серверу LDAP	
system ldap-server basedn	Указание базы поиска LDAP.

Команды настройки	
<отличительное_имя>	
system ldap-server dn <имя_привязки>	Указание отличительного имени (Bind DN), используемого для аутентификации при подключении к серверу LDAP.
system ldap-server groupbasedn <отличительное_имя>	Указание корневого объекта базы поиска групп LDAP.
system ldap-server host <узел>	Указание IP-адреса или символьного имени сервера LDAP.
system ldap-server netgroupbasedn <отличительное_имя>	Указание корневого объекта базы поиска сетевых групп LDAP.
system ldap-server nettimeout <время>	Установка ограничения на время ожидания
system ldap-server password <пароль>	Указание пароля, который используется для аутентификации при подключении к серверу LDAP.
system ldap-server port <порт>	Указание порта для подключения к серверу LDAP.
system ldap-server timeout <время>	Установить ограничение на время ожидания для операции поиска на сервере LDAP.
system ldap-server tls <режим>	Безопасное подключение к серверу LDAP с использованием SSL/TLS.
system ldap-server tls-server-auth <режим>	Включить/выключить авторизацию сервера LDAP.
system ldap-server userbasedn <отличительное_имя>	Установить корневой объект базы поиска пользователей LDAP.
Эксплуатационные команды	
clear arp address <ipv4-адрес>	Очистка кэша ARP системы для указанного IP-адреса.
clear arp interface <интерфейс>	Очистка кэша ARP системы для указанного интерфейса.
clear connection-tracking	Очистка всех подключений, отслеживаемых в данный момент.
clear console	Очистка консоли пользователя.
clear interfaces counters	Очистка счетчиков интерфейсов для всех интерфейсов.
flash init	Форматирование и монтирование флэш-накопителя в файловую систему, запись на него файла настройки с текущей конфигурацией устройства.
flash mount	Монтирование флэш-накопителя к системе.
flash umount	Отсоединение флэш-накопителя от системы.
geoip show <протокол_ip> <код_страны>	Отображение диапазонов ipv4- | ipv6-адресов для выбранного региона.
reboot	Перезагрузка системы.
show arp <интерфейс>	Отображение кэша ARP системы.
show dhcp leases	Отображение сведений о текущих выданных настроенным сервером DHCP адресах.
show dhcp client leases	Отображение сведений о текущих полученных клиентом DHCP адресах на указанном интерфейсе.
show disk <диск> format	Отображение сведений об указанном дисковом устройстве.
show files <каталог>	Отображение сведений о файлах.
show hardware cpu	Отображение сведений о системном процессоре.
show hardware dmi	Отображение сведений об интерфейсе DMI системы.
show hardware mem	Отображение сведений о памяти системы.
show hardware pci	Отображение сведений о шине PCI системы.
show history	Отображение журнала выполнения команд.
show host	Отображение сведений об узлах, достижимых для системы.
show interfaces	Отображение сведений о системных интерфейсах.
show interfaces stat <интерфейс>	Отображение статистики использования интерфейса
show reboot	Отображение даты и времени следующей запланированной перезагрузки.

Команды настройки	
show serial	Отображение сведений о серийном номере изделия.
show shutdown	Отображение даты и времени следующего запланированного выключения.
show snmp mib ifmib	Отображение сведения об интерфейсах из базы управляющей информации протокола SNMP.
show system boot-messages	Отображение сообщений, созданных ядром при загрузке.
show system connections	Отображение активных сетевых подключений в системе.
show system kernel-messages	Отображение сообщений в кольцевом буфере ядра.
show system memory	Отображение использования памяти системой.
show system processes	Отображение активных процессов в системе.
show system routing-daemons	Отображение активных служб маршрутизации.
show system sensors	Отображение сведений системных датчиков.
show system services	Отображение сведений об активных сетевых службах в системе.
show system storage	Отображение использования системных файлов системой и доступного места на накопителях.
show system uptime	Отображение сведений о длительности работы системы.
show system usb	Отображение сведений о периферийных устройствах, подключенных по шине USB.
show tech-support	Консолидированный отчет по сведениям о системе.
show version	Отображение сведений о сертификационной версии системного программного обеспечения.
shutdown	Завершение работы системы.
system back-up to <архив>	Полное сохранение состояния устройства в указанный архив.
system clean	Сброс конфигурации устройства в состояние по умолчанию.
system detect	Вывод информации об аппаратной платформе и модели устройства.
system restore from <архив>	Полное восстановление состояния устройства из архива.
system integrity export	Выгрузка на съемный флеш-носитель архива с файлами для расчета контрольных сумм.
terminal	Контроль за поведением системного терминала.
test	Выполнить регламентное тестирование.

Некоторые команды, относящиеся к конкретным функциям управления системой, описаны в других местах:

Сходные команды, описанные в других местах	
system date show;system date set	Команды для работы с системным временем.
system login	Команды управления пользователями описаны в разделе Управление пользователями
system management <состояние>	Включение/выключение управляющего интерфейса Numa Edge.
system syslog; clear log; dump log	Команды системной регистрации описаны в разделе Регистрация
system mail	Команды конфигурации почтового сервера описаны в разделе Регистрация
clear interfaces <интерфейс>	Команды очистки информации интерфейсов описаны подробно в разделе Настройка интерфейсов
clear ip; clear ipv6	Команды очистки статистики протоколов ipv4 и ipv6 описаны в разделе Статическая маршрутизация
clear nat	Команды очистки NAT описаны в разделе Преобразование сетевых адресов
clear https	Команда перезагрузки web-сервера описана в разделе Настройка доступа к web
named-list	Команды работы с именованными списками описаны в разделе Политика межсетевого экранирования
pki [import | import-pkcs12 | export |	Команды управления структурой открытых ключей описаны в

export-pkcs12 | update-crl]	разделе Инфраструктура открытых ключей
policy [clear | show]	Команды очистки статистики политик и отображения информации политик (соответствующие разделы)
routing [<протокол_маршрутизации> debug | table show]	Команды управления протоколами маршрутизации, просмотра таблиц маршрутизации (соответствующие разделы)
service <имя_сервиса> [show | restart | clear | renew]	Команды просмотра состояния и перезагрузки сервисов (соответствующие разделы)
show bridge	Команда просмотра информации о мостах описана в разделе Настройка интерфейсов
show incoming; show queueing	Команды просмотра информации о политиках ethernet описаны в разделе QoS

7.3.1 system country <код страны>

Указание двухзначного кода страны.

Синтаксис

```
set system country <код_страны>
delete system country
show system country
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   country код_страны
}
```

Параметры

код_страны

Двузначный код страны, в которой работает устройство.

Значение по умолчанию

По умолчанию установлено значение RU. Страна — Россия.

Указания по использованию

Эта команда используется для указания страны, в которой используется устройство Numa Edge.

Форма **set** этой команды используется для указания страны, в которой используется устройство Numa Edge.

Форма **delete** этой команды используется для удаления настройки и восстановления значения, принятого по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

7.3.2 system dns domain-name <домен>

Установка домена системы.

Синтаксис

```
set system dns domain-name <домен>
delete system dns domain-name
show system dns domain-name
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    dns {
        domain-name домен
    }
}
```

Параметры

домен

Обязательный. Домен, в котором находится система; например, "numa.ru". Формат - строка из букв, цифр, дефисов ("-") и одной точки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки домена системы.

ПРИМЕЧАНИЕ Параметры **domain-name** и **domain-search** не могут быть настроены одновременно - они являются взаимоисключающими.

Форма **set** этой команды используется для указания имени домена для использования системой.

Форма **delete** этой команды используется для удаления имени домена.

Форма **show** этой команды используется для просмотра настройки имени домена.

7.3.3 system dns domain-search domain <домен>

Определение набора доменов для автозавершения домена.

Синтаксис

```
set system dns domain-search domain <домен>
delete system dns domain-search domain <домен>
show system dns domain-search domain
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
  dns {
     domain-search {
         domain домен
     }
  }
}
```

Параметры

домен

Обязательный. Множественный узел. Имя домена для добавления в список доменов в строке порядка поиска или для удаления из этого списка. Формат - строка, указывающая домен; например, numatech.ru. Разрешены буквы, цифры, дефисы ("-") и одна точка (".").

Можно указать до 6 доменов, создав до 6 узлов `domain-search`.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для вывода списка из 6 или менее доменов для поиска при запросах на просмотр DNS.

Когда в систему приходит неполное имя узла, система пытается сформировать его полное доменное имя (FQDN) путем добавления доменов из этого списка к имени узла. Система пробует все имена доменов в том порядке, в котором они были настроены. Если ни одно из полученных полных доменных имен не является правильным, имя считается не разрешенным, и выдается сообщение об ошибке.

ПРИМЕЧАНИЕ Параметры **domain-name** и **domain-search** не могут быть настроены одновременно - они являются взаимоисключающими.

Форма **set** этой команды используется для добавления домена в список поиска. Обратите внимание, что **set** нельзя использовать для изменения имени домена в списке. Для замены неправильного домена следует удалить его и заменить новым.

Форма **delete** этой команды используется для удаления имени домена из списка.

Форма **show** этой команды используется для просмотра списка имен доменов.

7.3.4 system dns name-server <адрес>

Указание серверов имен DNS, доступных для системы.

Синтаксис

```
set system dns name-server <адрес> [domain <домен>]
delete system dns name-server <адрес> [domain <домен> | proto <протокол>]
show system dns name-server
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    dns {
        name-server адрес {
            domain домен
            proto протокол
        }
    }
}
```

Параметры

адрес

Множественный узел. IPv4-адрес сервера имен DNS для использования в локальных запросах имен.

домен

Имя домена, запросы для которого будут перенаправляться указанному серверу имён DNS.

протокол

Протокол, который будет использоваться при запросах к серверу имён DNS.

Допустимые значения:

dns: DNS протокол.

dot: DNS-over-TLS (DoT протокол).

doh: DNS-over-HTTPS (DoH протокол).

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания серверов доменных имен (DNS) для данной системы.

Форма **set** этой команды используется для определения сервера имен для данной системы. Обратите внимание, что с помощью команды **set** нельзя изменить элемент сервера имен DNS. Для замены элемента сервера имен следует удалить элемент и создать новый.

Форма **delete** этой команды используется для удаления сервера имен.

Форма **show** этой команды используется для просмотра списка определенных серверов имен.

7.3.5 system dns cache-size <размер>

Указание размера кэша службы ретрансляции DNS.

Синтаксис

```
set system dns cache-size <размер>
delete system dns cache-size
show system dns cache-size
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
system {
   dns {
      cache-size размер
   }
}
```

Параметры

размер

Максимальное число записей DNS, которое следует хранить в кэше ретрансляции DNS. Значение должно лежать в диапазоне от 0 до 10000, где 0 означает, что ограничение для числа хранимых записей отсутствует. Значение по умолчанию равно 150.

Значение по умолчанию

В кэше ретрансляции DNS хранится не более 150 записей DNS.

Указания по использованию

Эта команда используется для указания размера кэша службы ретрансляции DNS.

Форма **set** этой команды используется для установки размера кэша службы ретрансляции DNS.

Форма **delete** используется для восстановления значения по умолчанию для размера кэша службы ретрансляции DNS.

Форма **show** этой команды используется для просмотра установленного размера кэша для службы ретрансляции DNS.

ПРИМЕЧАНИЕ Если задействована поддержка DNSSEC, то значение cache-size не должно быть меньше 150.

7.3.6 system dns dnssec check-unsigned <состояние>

Проверка доменной зоны для неподписанного DNS-ответа.

Синтаксис

```
set system dns dnssec check-unsigned <состояние>
delete system dns dnssec check-unsigned <состояние>
show system dns dnssec check-unsigned
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   dns {
      dnssec {
         check-unsigned состояние
      }
   }
}
```

Параметры

состояние

Проверка доменной зоны для неподписанного DNS-ответа. Список допустимых значений:

enable: Разрешение проверки доменной зоны для неподписанного DNS-ответа.

disable: Запрет проверки доменной зоны для неподписанного DNS-ответа.

Значение по умолчанию

По умолчанию используется значение disable.

Указания по использованию

Эта команда используется для проверки доменной зоны для неподписанного DNS-ответа.

Форма **set** этой команды используется для проверки доменной зоны для неподписанного DNS-ответа.

Форма **delete** этой команды используется для удаления проверки доменной зоны для неподписанного DNS-ответа.

Форма **show** этой команды используется для просмотра настройки.

ПРИМЕЧАНИЕ В том случае, если для check-unsigned указано значение enable, но вышестоящий сервер службы DNS не поддерживает DNSSEC, сервис ретрансляции DNS не будет отвечать на запросы клиентов.

7.3.7 system dns dnssec disable

Отключение поддержки DNSSEC.

Синтаксис

```
set system dns dnssec disable
delete system dns dnssec disable
show system dns dnssec
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    dns {
        dnssec {
            disable
        }
    }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отключения поддержки DNSSEC.

Форма **set** этой команды используется для отключения поддержки DNSSEC.

Форма **delete** этой команды используется для отмены отключения поддержки DNSSEC.

Форма **show** этой команды используется для просмотра настройки.

7.3.8 system dns dnssec trust-anchor <имя>

Указание имени якоря доверия.

Синтаксис

```
set system dns dnssec trust-anchor <имя>
delete system dns dnssec trust-anchor <имя>
show system dns dnssec trust-anchor
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    dns {
        dnssec {
            trust-anchor имя
        }
    }
}
```

Параметры

имя

Имя якоря доверия.

Значение по умолчанию

Значения по умолчанию для якоря доверия соответствуют домену нулевого уровня.

Указания по использованию

Эта команда используется для указания имени якоря доверия.

Форма **set** этой команды используется для указания имени якоря доверия.

Форма **delete** этой команды используется для удаления указанного имени якоря доверия.

Форма **show** этой команды используется для просмотра настройки.

7.3.9 system dns dnssec trust-anchor <имя> algorithm <алгоритм>

Указание алгоритма подписи.

Синтаксис

```
set system dns dnssec trust-anchor <имя> algorithm <алгоритм>
delete system dns dnssec trust-anchor <имя> algorithm <алгоритм>
show system dns dnssec trust-anchor <имя> algorithm
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   dns {
      dnssec {
         trust-anchor имя {
            algorithm алгоритм
         }
      }
   }
}
```

Параметры

имя

Имя якоря доверия.

алгоритм

Алгоритм подписи. Возможные значения: rsa-sha1, rsa-sha1-nsec3, rsa-sha256, rsa-sha512, dsa-sha1, dsa-sha1-nsec3, gost2001, ecdsap256-sha256, ecdsap384-sha384.

Значение по умолчанию

По умолчанию используется алгоритм rsa-sha256.

Указания по использованию

Эта команда используется для указания алгоритма подписи.

Форма **set** этой команды используется для указания алгоритма подписи.

Форма **delete** этой команды используется для удаления указанного алгоритма подписи.

Форма **show** этой команды используется для просмотра настройки.

7.3.10 system dns dnssec trust-anchor <имя> digest <хеш>

Указание хеша

Синтаксис

```
set system dns dnssec trust-anchor <имя> digest <хеш>
delete system dns dnssec trust-anchor <имя> digest <хеш>
show system dns dnssec trust-anchor <имя> digest
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    dns {
        dnssec {
            trust-anchor имя {
                digest хеш
            }
        }
    }
}
```

Параметры

имя

Имя якоря доверия.

хеш

Хеш.

Значение по умолчанию

В том случае, если значение не задано, используется хеш домена нулевого уровня: 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5.

Указания по использованию

Эта команда используется для указания хеша.

Форма **set** этой команды используется для указания хеша.

Форма **delete** этой команды используется для удаления указанного хеша.

Форма **show** этой команды используется для просмотра настройки.

7.3.11 system dns dnssec trust-anchor <имя> digest-type <алгоритм_хеширования>

Указание алгоритма хеширования.

Синтаксис

```
set system dns dnssec trust-anchor <имя> digest-type <алгоритм_хеширования>
delete system dns dnssec trust-anchor <имя> digest-type <алгоритм_хеширования>
show system dns dnssec trust-anchor <имя>  digest-type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    dns {
        dnssec {
            trust-anchor имя {
                digest-type алгоритм_хеширования
            }
```

```
        }
    }
}
```

Параметры

имя

Имя якоря доверия.

алгоритм_хеширования

Алгоритм хеширования. Возможные значения: gost94, sha1, sha256, sha384.

Значение по умолчанию

По умолчанию используется алгоритм sha256.

Указания по использованию

Эта команда используется для указания алгоритма хеширования.

Форма **set** этой команды используется для указания алгоритма хеширования.

Форма **delete** этой команды используется для удаления указанного алгоритма хеширования.

Форма **show** этой команды используется для просмотра настройки.

7.3.12 system dns dnssec trust-anchor <имя> domain <домен>

Указание имени домена.

Синтаксис

```
set system dns dnssec trust-anchor <имя> domain <домен>
delete system dns dnssec trust-anchor <имя> domain <домен>
show system dns dnssec trust-anchor <имя>  domain
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    dns {
        dnssec {
            trust-anchor имя {
                domain домен
            }
        }
    }
}
```

Параметры

имя

Имя якоря доверия.

домен

Имя домена.

Значение по умолчанию

Домен нулевого уровня.

Указания по использованию

Эта команда используется для указания имени домена.

Форма **set** этой команды используется для указания имени домена.

Форма **delete** этой команды используется для удаления указанного имени домена.

Форма **show** этой команды используется для просмотра настройки.

7.3.13 system dns dnssec trust-anchor <имя> key-tag <маркер_ключа>

Указание маркера ключа.

Синтаксис

```
set system dns dnssec trust-anchor <имя> key-tag <маркер_ключа>
delete system dns dnssec trust-anchor <имя> key-tag <маркер_ключа>
show system dns dnssec trust-anchor <имя> key-tag
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   dns {
      dnssec {
         trust-anchor имя {
            key-tag маркер_ключа
         }
      }
   }
}
```

Параметры

имя

Имя якоря доверия.

маркер_ключа

Маркер ключа.

Значение по умолчанию

19036.

Указания по использованию

Эта команда используется для указания маркера ключа.

Форма **set** этой команды используется для указания маркера ключа.

Форма **delete** этой команды используется для удаления указанного маркера ключа.

Форма **show** этой команды используется для просмотра настройки.

7.3.14 system gateway-address <адрес>

Указание шлюза по умолчанию для системы.

Синтаксис

```
set system gateway-address <адрес>
delete system gateway-address
```

```
show system gateway-address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    gateway-address адрес
}
```

Параметры

адрес

Обязательный. IPv4-адрес шлюза по умолчанию.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки местоположения шлюза по умолчанию. Шлюз по умолчанию - это место, где маршрутизируются пакеты, если их получатель не соответствует ни одному из конкретных элементов маршрутизации. В одной системе может быть установлен только один шлюз по умолчанию.

Форма **set** этой команды используется для указания адреса шлюза по умолчанию.

Форма **delete** этой команды используется для удаления шлюза по умолчанию. Обратите внимание, что в большинстве случаев если шлюз по умолчанию не указан, то правильно маршрутизировать трафик не удается.

Форма **show** этой команды используется для просмотра адреса шлюза по умолчанию.

7.3.15 system host-name <имя>

Установка имени узла для системы.

Синтаксис

```
set system host-name <имя>
delete system host-name
show system host-name
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    host-name имя
}
```

Параметры

имя

Имя, которое нужно дать системе. Допускаются только буквы, цифры и дефисы ("-").

Значение по умолчанию

По умолчанию имя узла предварительно настроено как "edge". При удалении имени узла или при удалении узла конфигурации system восстанавливается значение по умолчанию.

Указания по использованию

Эта команда используется для указания имени узла для системы.

После установки этого значения вид запроса на ввод команд изменяется в соответствии с новым именем узла. Чтобы увидеть изменение запроса на ввод команд, следует выйти из системы и вновь в нее войти.

Форма **set** этой команды используется для изменения имени узла.

Форма **delete** этой команды используется для восстановления имени узла по умолчанию ("edge").

Форма **show** этой команды используется для просмотра настройки имени узла.

7.3.16 system options reboot-on-panic <режим>

Установка поведения системы в случае неисправимой ошибки.

Синтаксис

```
set system options reboot-on-panic <режим>

delete system options reboot-on-panic

show system options reboot-on-panic
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   options {
      reboot-on-panic режим
   }
}
```

Параметры

режим

Обязательный. Указывает, будет ли система перезагружаться автоматически в случае неисправимой ошибки ядра. Поддерживаются следующие значения:

true: Система перезагружается в случае неисправимой ошибки ядра.

false: Система не перезагружается в случае неисправимой ошибки ядра.

Значение по умолчанию

По умолчанию система перезагружается в случае неисправимой ошибки ядра.

Указания по использованию

Настройка системы на отсутствие перезагрузки при неисправимой ошибке ядра позволяет пользователю исследовать сведения, которые могут быть полезными при определении причины неисправимой ошибки.

Форма **set** этой команды используется для указания необходимости перезагрузки при неисправимой ошибке ядра.

Форма **delete** этой команды используется для восстановления значения по умолчанию для этого режима.

Форма **show** этой команды используется для просмотра настройки для этого режима.

7.3.17 system static-host-mapping host-name <имя>

Определение статического сопоставления между именем узла и IP-адресом.

Синтаксис

```
set system static-host-mapping host-name <имя> [inet <адрес> | alias <псевдоним>]

delete system static-host-mapping host-name <имя> [inet | alias]

show system static-host-mapping host-name <имя> [inet | alias]
```

Режим интерфейса
Режим настройки.

Ветвь конфигурации
```
system {
    static-host-mapping {
        host-name имя {
            inet адрес          alias псевдоним
        }
    }
}
```

Параметры
имя

Множественный узел. Полное доменное имя (FQDN), статически сопоставляемое с IP-адресом (например, router1.mydomain.com). Допускаются только буквы, цифры, точки (".") и дефисы ("-"). Можно определить несколько сопоставлений, создав несколько узлов конфигурации host-name.

адрес

Обязательный. IPv4-адрес или IPv6-адрес, статически сопоставляемый с именем узла.

псевдоним

Необязательный. Множественный узел. Псевдоним для адреса. Допускаются буквы, цифры и дефисы. Для узла можно определить несколько псевдонимов, создав несколько узлов конфигурации alias.

Значение по умолчанию
Отсутствует.

Указания по использованию
Эта команда используется для статического сопоставления имени узла и IP-адреса и одного или большего числа псевдонимов.

Форма **set** этой команды используется для создания нового статического сопоставления между именем узла и IP-адресом, назначения адреса или указания псевдонима.

Форма **delete** этой команды используется для удаления статического сопоставления, адреса или псевдонима.

Форма **show** этой команды используется для просмотра статического сопоставления, адреса или псевдонима.

7.3.18 system static-host-mapping local-ttl <время_жизни>

Установка периода времени, в течение которого клиент будет считать полученную информацию о сопоставлении актуальной.

Синтаксис
```
set system static-host-mapping local-ttl <время_жизни>
delete system static-host-mapping local-ttl
show system static-host-mapping local-ttl
```

Режим интерфейса
Режим настройки.

Ветвь конфигурации
```
system {
    static-host-mapping {
```

```
        local-ttl время_жизни
    }
}
```

Параметры

время_жизни

Указывает период времени в секундах, в течение которого клиент будет считать полученную информацию актуальной. Значение должно лежать в диапазоне 60-259200 (3 дня).

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания периода вермени, в течение которого клиент будет считать актуальной полученную информацию о сопоставлении. Данная опция позволяет снизить нагрузку на сервер, ввиду того что полученный ответ будет закэширован на стороне клиента на указанный период времени.

Форма **set** этой команды используется для создания нового статического сопоставления между именем узла и IP-адресом, назначения адреса или указания псевдонима.

Форма **delete** этой команды используется для удаления статического сопоставления, адреса или псевдонима.

Форма **show** этой команды используется для просмотра статического сопоставления, адреса или псевдонима.

7.3.19 system time-zone <часовой_пояс>

Установка часового пояса для локальных часов системы.

Синтаксис

```
set system time-zone <часовой_пояс>
delete system time-zone
show system time-zone
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
     time-zone часовой_пояс
}
```

Параметры

часовой_пояс

Строка, обозначающая часовой пояс. Ее основной формат: Регион/Местоположение. Например, Europe/Paris. Для отображения различных вариантов следует использовать автозавершение команд (т.е. клавишу <Tab>).

Значение по умолчанию

Значение по умолчанию Europe/Moscow.

Указания по использованию

Эта команда используется для установки часового пояса для локальных часов системы.

В дополнение к широкому кругу доступных пар регион/местоположение, поддерживается обратная совместимость при помощи формата Etc/<сдвиг> вместо регион/местоположение. Обратите внимание, что в записи Etc/<сдвиг> используется сдвиг в формате Posix. Это значит, что положительный сдвиг используется для

указания региона к западу от Гринвича, а не к востоку от Гринвича, как во многих системах. Например, Etc/GMT+8 соответствует 8 часам позади UTC (то есть к западу от Гринвича).

Форма **set** этой команды используется для установки часового пояса в первый раз или для изменения установленного часового пояса.

Форма **delete** этой команды используется для удаления установленного часового пояса.

Форма **show** этой команды используется для просмотра установленного часового пояса.

7.3.20 system watchdog

Установка режима работы сторожевого таймера.

Синтаксис

```
set system watchdog [check <сервис> | timeout <время>]
delete system watchdog [check | timeout]
show system watchdog
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   watchdog {
      check сервис
      timeout время
   }
}
```

Параметры

сервис

Сервис, который будет отслеживаться сторожевым таймером. Допустимые значения представлены в таблице ниже.

Таблица 13– Сервисы, доступные для отслеживания

Значение	Описание
ftpproxy	FTP прокси-сервер
https	Удалённый доступ через web
socksproxy	SOCKS прокси-сервер
ssh	Удаленный доступ через SSH
syslog	Системный журнал
telnet	Удаленный доступ через Telnet
token-auth	Локальная аутентификация на токене
watcher	Сервис проверки изменений файлов
wifi-ap	Сервис точки доступа Wi-Fi

время

Время ожидания в секундах. Значение должно лежать в диапазоне 30-255.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки режима работы сторожевого таймера.

Форма **set** этой команды позволяет указать параметры работы сторожевого таймера.

Форма **delete** этой команды используется для удаления настройки.

Форма **show** этой команды используется для отображения настройки.

7.3.21 system ip arp table-size <размер>

Указание максимального количества записей, которые хранятся в кэше ARP.

Синтаксис

```
set system ip arp table-size <размер>
delete system ip arp table-size
show system ip arp table-size
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   ip{
      arp {
         table-size размер
      }
   }
}
```

Параметры

размер

Максимальное количество записей, которые хранятся в кэше ARP. Допустимые значения: 1024, 2048, 4096, 8192, 16384.

Значение по умолчанию

По умолчанию размер таблицы составляет 1024 записи.

Указания по использованию

Эта команда используется для указания максимального количества записей в кэше ARP. Это жесткое ограничение, указанное значение никогда не будет превышено. При достижении указанного числа записей, автоматически запускается сборщик мусора.

Форма **set** этой команды используется для установки максимального количества записей в кэше ARP.

Форма **delete** этой команды используется для удаления установленного значения и восстановления значения, принятого по умолчанию.

Форма **show** этой команды используется для просмотра установленного значения.

7.3.22 system ip disable-forwarding

Установка запрета на перенаправление IPv4-пакетов для всех интерфейсов.

Синтаксис

```
set system ip disable-forwarding
delete system ip disable-forwarding
show system ip disable-forwarding
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   ip {
      disable-forwarding
   }
}
```

Параметры

Отсутствует.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки запрета на перенаправление IPv4-пакетов для всех интерфейсов.

Форма **set** этой команды используется для установки запрета на перенаправление IPv4-пакетов.

Форма **delete** этой команды используется для снятия запрета на перенаправление IPv4-пакетов.

Форма **show** этой команды используется для просмотра установленного значения.

7.3.23 system ipv6 disable

Установка запрета на присвоение IPv6-адресов для всех интерфейсов.

Синтаксис

```
set system ipv6 disable
delete system ipv6 disable
show system ipv6 disable
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   ipv6 {
      disable   }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется запрета присвоения IPv6-адресов для всех интерфейсов. При этом стек протокола IPv6 присутствует в системе. IPv6-пакеты системой не обрабатываются.

Форма **set** этой команды используется для установки запрета на присвоение IPv6- адресов.

Форма **delete** этой команды используется для снятия запрета на присвоение IPv6- адресов.

Форма **show** этой команды используется для просмотра установленного значения.

7.3.24 system ipv6 disable-forwarding

Запрет перенаправления IPv6-пакетов на всех интерфейсах.

Синтаксис

```
set system ipv6 disable-forwarding

delete system ipv6 disable-forwarding

show system ipv6 disable-forwarding
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   ipv6 {
      disable-forwarding   }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для запрета перенаправления IPv6-пакетов на всех интерфейсах. При этом сохраняются все настройки IPv6-протокола и все выданные IPv6-адреса.

Форма **set** этой команды используется для установки запрета перенаправления IPv6-пакетов.

Форма **delete** этой команды используется для снятия запрета перенаправления IPv6-пакетов.

Форма **show** этой команды используется для просмотра установленного значения.

7.3.25 system ipv6 neighbor table-size <размер>

Указание максимального количества записей, которые хранятся в таблице соседей IPv6.

Синтаксис

```
set system ipv6 neighbor table-size <размер>

delete system ipv6 neighbor table-size

show system ipv6 neighbor table-size
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   ipv6 {
      neighbor {
         table-size размер
      }
   }
}
```

Параметры

размер

Максимальное количество записей, которые хранятся в таблице соседей IPv6. Допустимые значения: 1024, 2048, 4096, 8192, 16384.

Значение по умолчанию

По умолчанию размер таблицы составляет 1024 записи.

Указания по использованию

Эта команда используется для указания максимального количества записей в таблице соседей IPv6. Это жесткое ограничение, указанное значение никогда не будет превышено. При достижении указанного числа записей, автоматически запускается сборщик мусора.

Форма **set** этой команды используется для установки максимального количества записей в таблице соседей IPv6.

Форма **delete** этой команды используется для удаления установленного значения и восстановления значения, принятого по умолчанию.

Форма **show** этой команды используется для просмотра установленного значения.

7.3.26 system ipv6 strict-dad

Включение блокировки IPv6-протокола на интерфейсе после обнаружения дублирующего link-local адреса (MAC адреса интерфейса Ethernet) с помощью протокола определения дублирующего адреса (Duplicate Address Detection – DAD).

Синтаксис

```
set system ipv6 strict-dad

delete system ipv6 strict-dad

show system ipv6 strict-dad
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   ipv6 {
      strict-dad   }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для включения блокировки IPv6-протокола на интерфейсе после обнаружения дублирующего link-local-адреса с помощью протокола DAD.

Форма **set** этой команды используется для включения возможности блокировки IPv6 интерфейсе после обнаружения дублирующего link-local-адреса.

Форма **delete** этой команды используется для удаления установленного значения и восстановления значения, принятого по умолчанию.

Форма **show** этой команды используется для просмотра установленного значения.

7.3.27 system ssh cipher <алгоритм>

Указание допустимых для использования клиентом SSH алгоритмов шифрования.

Синтаксис

```
set system ssh cipher <алгоритм>

delete system ssh cipher <алгоритм>

show system ssh cipher
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
system {
    ssh {
        cipher алгоритм
    }
}
```

Параметры

алгоритм

Допустимый для использования клиентом SSH алгоритм шифрования. Множественный узел.

Список поддерживаемых алгоритмов:

- **aes128-cbc, aes128-ctr** - AES (Advanced Encryption Standard) с ключом 128 бит;
- **aes192-cbc, aes192-ctr** - AES (Advanced Encryption Standard) с ключом 192 бит;
- **aes256-cbc, aes256-ctr** - AES (Advanced Encryption Standard) с ключом 256 бит;
- **arcfour** - Alleged RC4 с ключом 128 бит;
- **arcfour128, arcfour256** - Alleged RC4 с ключом 128 / 256 бит (с дополнениями RFC 4345);
- **blowfish-cbc** - Blowfish с ключом 128 бит;
- **cast128-cbc** - CAST-128 с ключом 128 бит;
- **gost89-cbc, gost89-ctr, gost89-cfb, gost89-ofb** - шифрование на основе алгоритма, определенного ГОСТ 28147-89;
- **kuznechik-cbc, kuznechik-ctr, kuznechik-cfb, kuznechik-ofb** - шифрование на основе алгоритма "Кузнечик" (ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015).

Значение по умолчанию

По умолчанию в изделии настроен алгоритм kuznechik-ofb.

Указания по использованию

Эта команда используется для указания допустимых для использования клиентом SSH алгоритмов симметричного шифрования.

Форма **set** этой команды позволяет разрешить использование того или иного алгоритма шифрования для клиента SSH. Возможно задание нескольких поддерживаемых алгоритмов.

Форма **delete** этой команды используется для запрещения использования того или иного алгоритма для клиента SSH.

Форма **show** этой команды используется для просмотра настройки.

7.3.28 system ssh hmac <алгоритм>

Указание допустимых алгоритмов выработки имитовставки для клиента SSH.

Синтаксис

```
set system ssh hmac <алгоритм>

delete system ssh hmac <алгоритм>

show system ssh hmac
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
system {
    ssh {
        hmac алгоритм
    }
}
```

Параметры

алгоритм

Допустимый для использования клиентом SSH алгоритм выработки имитовставки. Множественный узел.

Список поддерживаемых алгоритмов:

- **hmac-md5** - алгоритм MD5 (Message Digest) с хешем 128 бит;
- **hmac-md5-96** - алгоритм на основе MD5 с хешем 96 бит;
- **hmac-sha1** - алгоритм SHA1 (Secure Hash Algorithm) с хешем 128 бит;
- **hmac-sha1-96** - алгоритм на основе SHA1 с хешем 96 бит;
- **hmac-ripemd160** - алгоритм RIPEMD (RACE Integrity Primitives Evaluation Message Digest) с хешем 160 бит;
- **hmac-ripemd160@openssh.com** - алгоритм RIPEMD с хешем 160 бит в реализации проекта OpenSSH;
- **umac-64@openssh.com** - алогритм UMAC (universal hashing);
- **hmac-gosthash** - алгоритм на основе ГОСТ Р 34.11-94;
- **hmac-stribog-256, hmac-stribog-512** - алгоритм на основе ГОСТ Р 34.11-2012 с хешем 256 / 512 бит соответственно.

Значение по умолчанию

По умолчанию в изделии настроены алгоритмы hmac-stribog-256 и hmac-stribog-512.

Указания по использованию

Эта команда используется для указания допустимых для использования алгоритмов выработки имитовставки.

Форма **set** этой команды позволяет разрешить использование того или иного алгоритма выработки имитовставки. Возможно задание нескольких поддерживаемых алгоритмов.

Форма **delete** этой команды используется для запрещения использования того или иного алгоритма выработки имитовставки.

Форма **show** этой команды используется для просмотра настройки.

7.3.29 system ssh key-exchange-algo <алгоритм>

Указание допустимых алгоритмов обмена ключами для клиента SSH.

Синтаксис

```
set system ssh key-exchange-algo <алгоритм>
delete system ssh key-exchange-algo <алгоритм>
show system ssh key-exchange-algo
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
system {
    ssh {       key-exchange-algo алгоритм
```

```
}}
```

Параметры

алгоритм

Допустимый для использования клиентом SSH алгоритм обмена ключами. Множественный узел.

Список поддерживаемых алгоритмов:

- diffie-hellman-group-exchange-sha1;
- diffie-hellman-group-exchange-sha256;
- diffie-hellman-group1-sha1;
- diffie-hellman-group14-sha1;
- ecdh-gost2012-256-cpa;
- ecdh-gost2012-256-cpb.

Значение по умолчанию

По умолчанию используются алгоритм ecdh-gost2012-256-cpa.

Указания по использованию

Эта команда позволяет указать допустимые алгоритмы ключевого обмена.

Форма **set** этой команды позволяет разрешить использование того или иного алгоритма ключевого обмена. Возможно задание нескольких поддерживаемых алгоритмов.

Форма **delete** этой команды используется для запрещения использования того или иного алгоритма ключевого обмена.

Форма **show** этой команды используется для просмотра настройки.

7.3.30 system ssh hostkey-algo <алгоритм>

Указание допустимых алгоритмов асимметричного шифрования для клиента SSH.

Синтаксис

```
set system ssh hostkey-algo <алгоритм>

delete system ssh hostkey-algo <алгоритм>

show system ssh hostkey-algo
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
system {
   ssh {
      hostkey-algo <алгоритм>
   }
}
```

Параметры

алгоритм

Допустимый для использования клиентом SSH алгоритм асимметричного шифрования (используется для аутентификации). Множественный узел.

Список поддерживаемых алгоритмов:

- ecdsa-sha2-nistp256;
- rsa-sha2-256;
- rsa-sha2-512;

- ssh-ed25519;
- ssh-gost2012-256-cpa;
- ssh-gost2012-512-tc26a;
- ssh-rsa.

Значение по умолчанию

По умолчанию используются алгоритмы ssh-gost2012-256-cpa и ssh-gost2012-512-tc26a.

Указания по использованию

Эта команда позволяет указать допустимые алгоритмы асимметричного шифрования (используется для аутентификации).

Форма **set** этой команды позволяет разрешить использование того или иного алгоритма асимметричного шифрования. Возможно задание нескольких поддерживаемых алгоритмов.

Форма **delete** этой команды используется для запрещения использования того или иного алгоритма асимметричного шифрования.

Форма **show** этой команды используется для просмотра настройки.

7.3.31 system ldap-server basedn <отличительное_имя>

Указание базы поиска LDAP.

Синтаксис

```
set system ldap-server basedn <отличительное_имя>
delete system ldap-server basedn
show system ldap-server basedn
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   ldap-server {
      basedn отличительное_имя
   }
}
```

Параметры

отличительное_имя

Обязательный. Отличительное имя базы поиска LDAP. Отличительное имя должно быть указано в формате, определенном в RFC 2253. Например: dc=example,dc=com.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать базу поиска LDAP.

Форма **set** данной команды позволяет указать отличительное имя.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

7.3.32 system ldap-server dn <имя_привязки>

Указание имени привязки (Bind DN), используемого для аутентификации при подключении к серверу LDAP.

Синтаксис

```
set system ldap-server dn <имя_привязки>

delete system ldap-server dn

show system ldap-server dn
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    ldap-server {
        dn имя_привязки
     }
}
```

Параметры

имя_привязки

Обязательный. Имя привязки (bind DN), которое будет использоваться для аутентификации при подключении к серверу LDAP. Имя привязки представляет собой отличительное имя, которое должно быть указано в формате, определенном в RFC 2253. Например: cn=adm,dc=example,dc=com.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать отличительное имя, которое будет использоваться при аутентификации клиента на сервере LDAP.

Для того чтобы иметь возможность работы со службой каталога, клиент должен пройти обязательную аутентификацию на сервере LDAP. Указанное отличительное имя (Distinguished Name) должно находиться в пространстве имен, описываемых каталогом.

Форма **set** данной команды позволяет указать отличительное имя для аутентификации при подключении к серверу LDAP.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

7.3.33 system ldap-server groupbasedn <отличительное_имя>

Указание корневого объекта базы поиска групп LDAP.

Синтаксис

```
set system ldap-server groupbasedn <отличительное_имя>

delete system ldap-server groupbasedn

show system ldap-server groupbasedn
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    ldap-server {
        groupbasedn отличительное_имя
    }
```

```
}
```

Параметры

отличительное_имя

Обязательный. Отличительное имя корневого объекта, начиная от которого будет осуществляться поиск групп LDAP. Отличительное имя должно быть указано в формате, определенном в RFC 2253. Например: ou=groups,dc=example,dc=com.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать отличительное имя корневого объекта, начиная от которого будет осуществляться поиск групп LDAP.

Форма **set** данной команды позволяет указать отличительное имя.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

7.3.34 system ldap-server host <узел>

Указание IP-адреса или символьного имени сервера LDAP.

Синтаксис

```
set system ldap-server host <узел>
delete system ldap-server host
show system ldap-server host
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   ldap-server {
      host узел
   }
}
```

Параметры

узел

Обязательный. Сервер LDAP, к которому будет осуществляться подключение. Допустимые значения представлены в таблице ниже.

Таблица 14– Формат указания сервера LDAP.

Значение	Описание
<x.x.x.x>	IPv4-адрес сервера LDAP.
<h:h:h:h:h:h>	IPv6-адрес сервера LDAP.
<text>	Символьное имя сервера LDAP.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать IP-адрес или символьное имя сервера LDAP, к которому будет осуществляться подключение.

Форма **set** данной команды используется для указания IP-адреса сервера LDAP.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

7.3.35 system ldap-server netgroupbasedn <отличительное_имя>

Указание корневого объекта базы поиска сетевых групп LDAP.

Синтаксис

```
set system ldap-server netgroupbasedn <отличительное_имя>
delete system ldap-server netgroupbasedn
show system ldap-server netgroupbasedn
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   ldap-server {
      netgroupbasedn отличительное_имя
   }
}
```

Параметры

отличительное_имя

Отличительное имя корневого объекта, начиная от которого будет осуществляться поиск сетевых групп LDAP. Отличительное имя должно быть указано в формате, определенном в RFC 2253. Например: ou=netgroups,dc=example,dc=com.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать отличительное имя корневого объекта, начиная от которого будет осуществляться поиск групп LDAP.

Форма **set** данной команды позволяет указать отличительное имя.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

7.3.36 system ldap-server nettimeout <время>

Установить максимальный интервал времени ожидания для всех сетевых взаимодействий с сервером LDAP.

Синтаксис

```
set system ldap-server nettimeout <время>
delete system ldap-server nettimeout
show system ldap-server nettimeout
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    ldap-server {
        nettimeout время
    }
}
```

Параметры

время

Максимальный интервал времени ожидания, в секундах, для всех сетевых взаимодействий с сервером LDAP. Значение должно лежать в диапазоне 5-360.

Значение по умолчанию

По умолчанию максимальное время ожидания равно 10 секундам.

Указания по использованию

Данная команда позволяет установить максимальное время ожидания для всех сетевых взаимодействий с сервером LDAP.

Форма **set** данной команды используется для установки максимального времени ожидания.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

7.3.37 system ldap-server password <пароль>

Указание пароля, который используется для аутентификации при подключении к серверу LDAP.

Синтаксис

```
set system ldap-server password <пароль>
delete system ldap-server password
show system ldap-server password
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    ldap-server {
        password пароль
    }
}
```

Параметры

пароль

Обязательный. Пароль, который используется для аутентификации при подключении к серверу LDAP.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать пароль, который используется для аутентификации при подключении к серверу LDAP.

Форма **set** данной команды используется для указания пароля.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

7.3.38 system ldap-server port <порт>

Указание номера сетевого порта для подключения к серверу LDAP.

Синтаксис

```
set system ldap-server port <порт>
delete system ldap-server port
show system ldap-server port
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   ldap-server {
      port порт
   }
}
```

Параметры

порт

Обязательный. Номер сетевого порта для подключения к серверу LDAP.

Значение по умолчанию

По умолчанию используется сетевой порт 389.

Указания по использованию

Данная команда позволяет указать номер сетевого порта, который будет использоваться при подключении к серверу LDAP.

Форма **set** данной команды позволяет указать номер сетевого порта, используемого при подключении к серверу LDAP.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** используется для отображения настройки.

7.3.39 system ldap-server timeout <время>

Установить максимальное время ожидания для операции поиска на сервере LDAP.

Синтаксис

```
set system ldap-server timeout <время>
delete system ldap-server timeout
show system ldap-server timeout
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   ldap-server {
      timeout время
```

```
    }
}
```

Параметры

время

Максимальный интервал времени, в секундах, в течение которого ожидается окончание операции поиска на сервере LDAP.

Значение по умолчанию

По умолчанию установлено максимальное время ожидания окончания операции поиска равное 15 секундам.

Указания по использованию

Данная команда позволяет установить максимальное время ожидания окончания операции поиска на сервере LDAP.

Форма **set** данной команды используется для указания максимального времени окончания операции поиска на сервере LDAP.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

7.3.40 system ldap-server tls <режим>

Использовать режим TLS для подключения к серверу LDAP.

Синтаксис

```
set system ldap-server tls <режим>
delete system ldap-server
show system ldap-server
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    ldap-server {
      tls режим
    }
}
```

Параметры

режим

Устанавливает подключения к серверу LDAP. Список допустимых значений:

enable: Подключение к серверу LDAP с использованием режима TLS.

disable: Подключение к серверу LDAP без использования режима TLS.

Значение по умолчанию

По умолчанию режим TLS не используется.

Указания по использованию

Данная команда позволяет включить/отключить использование режима TLS при подключении к LDAP.

Протокол TLS предоставляет возможности аутентификации, обеспечения конфиденциальности и целостности передаваемой информации с использованием криптографических средств. При включении режима TLS взаимодействие с сервером LDAP будет осуществляться с использованием STARTTLS.

ПРИМЕЧАНИЕ Для корректной работы TLS символьное имя сервера LDAP должно совпадать с именем (CN), указанным в сертификате сервера. (Указанное символьное имя должно корректно разрешаться при помощи DNS.) В случае несовпадения символьного имени сервера LDAP и имени, указанного в сертификате сервера, соединение установлено не будет.

Форма **set** данной команды позволяет включить/отключить использование TLS при подключении к серверу LDAP.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

7.3.41 system ldap-server tls-server-auth <режим>

Включить/выключить авторизацию сервера LDAP.

Синтаксис

```
set system ldap-server tls-server-auth <режим>
delete system ldap-server tls-server-auth
show system ldap-server tls-server-auth
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
  ldap-server {
      tls-server-auth режим
   }
}
```

Параметры

режим

Режим подключения к серверу LDAP. Список допустимых значений:

enable: Авторизация сервера LDAP используется.

disable: Авторизация сервера LDAP не используется.

Значение по умолчанию

По умолчанию авторизация сервера LDAP используется.

Указания по использованию

Данная команда позволяет включить/отключить авторизацию сервера LDAP.

При включенной авторизации при установке подключения к серверу LDAP будет осуществляться проверка сертификата сервера LDAP. Проверка будет пройдена успешно, если сертификат сервера LDAP подписан удостоверяющим центром, известным модулю PKI.

ПРИМЕЧАНИЕ Для корректной работы TLS символьное имя сервера LDAP должно совпадать с именем (CN), указанным в сертификате сервера. (Указанное символьное имя должно корректно разрешаться при помощи DNS.) В случае несовпадения символьного имени сервера LDAP и имени, указанного в сертификате сервера, соединение установлено не будет.

Форма **set** данной команды позволяет включить/отключить использование авторизации сервера LDAP.

Форма **delete** данной команды используется для удаления настройки и восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки.

7.3.42 system ldap-server userbasedn <отличительное_имя>

Установить корневой объект базы поиска пользователей LDAP.

Синтаксис

```
set system ldap-server userbasedn <отличительное_имя>
delete system ldap-server userbasedn
show system ldap-server userbasedn
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   ldap-server {
      userbasedn отличительное_имя
   }
}
```

Параметры

отличительное_имя

Обязательный. Отличительное имя корневого объекта, начиная от которого будет осуществляться поиск пользователей LDAP. Отличительное имя должно быть указано в формате, определенном в RFC 2253, например, ou=users,dc=example,dc=com.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать корневой объект, начиная от которого будет осуществляться поиск пользователей в каталоге.

Форма **set** данной команды позволяет указать отличительное имя корневого объекта.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

7.3.43 clear arp address <ipv4-адрес>

Очистка кэша ARP системы для указанного IPv4-адреса.

Синтаксис

```
clear arp address ipv4-адрес
```

Режим интерфейса

Эксплуатационный режим.

Параметры

ipv4-адрес

Удаление элемента ARP для указанного IP-адреса из кэша ARP.

Значение по умолчанию
Отсутствует.

Указания по использованию
Эта команда используется для удаления элементов ARP, связанных с конкретным IP-адресом, из кэша ARP.

7.3.44 clear arp interface <интерфейс>

Очистка кэша ARP системы для указанного интерфейса.

Синтаксис
clear arp interface интерфейс

Режим интерфейса
Эксплуатационный режим.

Параметры
интерфейс

Очистка всего кэша ARP для указанного интерфейса. Интерфейс должен быть заранее настроен в системе.

Значение по умолчанию
Отсутствует.

Указания по использованию
Эта команда используется для удаления элементов ARP, связанных с интерфейсом, из кэша ARP.

7.3.45 clear connection-tracking

Очистка всех подключений, отслеживаемых в данный момент.

Синтаксис
```
clear connection-tracking
```

Режим интерфейса
Эксплуатационный режим.

Параметры
Отсутствуют.

Значение по умолчанию
Отсутствует.

Указания по использованию
Эта команда используется для очистки всех подключений, отслеживаемых в данный момент.

7.3.46 clear console

Очистка консоли пользователя.

Синтаксис
```
clear console
```

Режим интерфейса
Эксплуатационный режим.

Параметры
Отсутствуют.

Значение по умолчанию
Отсутствует.

Указания по использованию
Эта команда используется для очистки экрана консоли.

7.3.47 clear interfaces counters

Очистка счетчиков интерфейсов для всех интерфейсов.

Синтаксис
```
clear interfaces [<тип_интерфейса> [<интерфейс>]] counters
```

Режим интерфейса
Эксплуатационный режим.

Параметры
тип_интерфейса

Тип интерфейсов, для которых необходимо очистить счетчики. Допустимые значения представлены в таблице ниже:

Таблица 15 – Допустимые типы интерфейсов

Значение	Описание
Bonding	Интерфейсы агрегированных каналов
Bridge	Интерфейсы моста
Ethernet	Интерфейсы ethernet
Loopback	Интерфейсы заглушки
Multilink	Интерфейсы multilink
Ppp	Интерфейсы канального уровня
pseudo-ethernet	Интерфейсы pseudo-ethernet
Serial	Последовательные интерфейсы
tunnel	Туннельные интерфейсы

интерфейс

Имя конкретного интерфейса, для которого следует очистить счетчики.

Значение по умолчанию
Отсутствует.

Указания по использованию
Эта команда используется для очистки счетчиков для всех интерфейсов всех типов. Имеется возможность указать конкретный тип интерфейса или конкретный интерфейс воспользовавшись системой автодополнения. Просмотреть значения счетчиков можно при помощи команды `show interfaces counters`.

7.3.48 flash init

Форматирование флэш-накопителя и подготовка его для записи файла настройки.

Синтаксис
```
flash init
```

Режим интерфейса
Эксплуатационный режим.

Параметры
Отсутствуют.

Значение по умолчанию
Отсутствует.

Указания по использованию
Эта команда используется для форматирования флэш-накопителя.

Система записывает файловую систему на флэш-накопитель и делает ее доступной для системы Numa Edge. Кроме того, она записывает копию работающей настройки в файл **/media/hdd/config/config.boot**.

В результате инициализации флэш-накопителя все ранее находившиеся на нем данные стираются. Система напоминает пользователю об этом и дает 5-секундный интервал времени, во время которого можно закрыть команду, введя "n" в ответ на запрос "Continue (y/n)? [y]" или нажав сочетание клавиш <Ctrl>+C.

После форматирования флэш-накопителя файл config.boot сохраняется на нее автоматически. Кроме того, файл настройки config.boot можно сохранить на диск с помощью команды `save`.

Примеры
В примере выполняется подготовка флэш-накопителя для записи файла настройки и запись работающей настройки в файл **/media/hdd/config/config.boot**.

Пример 40– Инициализация флэш-накопителя для записи файлов настройки

```
admin@edge:~$ flash init
This will erase all data on /dev/usbstick.
Your configuration was saved in: /media/hdd/config/config.boot
admin@edge:~$
```

7.3.49 flash mount

Монтирует флэш-накопитель к системе Numa Edge.

Синтаксис
`flash mount`

Режим интерфейса
Эксплуатационный режим.

Параметры
Отсутствуют.

Значение по умолчанию
Отсутствует.

Указания по использованию
Эта команда используется для монтирования флэш-накопителя.

Монтируется флэш-накопитель, что делает его доступным для системы Numa Edge по расположению **/media/hdd/**.

7.3.50 flash umount

Отсоединение флэш-накопителя от системы Numa Edge.

Синтаксис
`flash umount`

Режим интерфейса
Эксплуатационный режим.

Параметры
Отсутствуют.

Значение по умолчанию
Отсутствует.

Указания по использованию
Эта команда используется для отсоединения флэш-накопителя.

Отсоединяется флэш-накопитель, что делает его недоступным для системы Numa Edge по расположению **/media/hdd/.**

7.3.51 geoip show <протокол_ip> <код_страны>

Отображение диапазонов адресов указанного протокола ip для выбранного региона.

Синтаксис
```
geoip show <протокол_ip> <код_страны>
```

Режим интерфейса
Эксплуатационный режим.

Параметры
протокол_ip

Версия протокола IP (IPv4 или IPv6).

код_страны

Код страны из предлагаемого списка в виде двух букв в верхнем регистре.

Примеры
В примере показан частичный вывод команды geoip show ipv4 RU.

Пример 41– Отображение диапазона адресов протокола ipv4 для России.

```
admin@edge:~$ geoip show ipv4 RU
2.60.0.0    - 2.63.255.255
2.92.0.0    - 2.95.255.255
5.1.48.0    - 5.1.55.255
5.2.32.0    - 5.2.63.255
5.3.0.0     - 5.3.255.255
5.8.0.0     - 5.8.23.255
5.8.28.0    - 5.8.31.255
5.8.36.0    - 5.8.39.255
5.8.48.0    - 5.8.62.255
5.8.64.0    - 5.8.67.255
5.8.72.0    - 5.8.87.255
5.8.92.0    - 5.8.95.255
5.8.160.0   - 5.8.183.255
5.8.192.0   - 5.8.239.255
5.11.64.0   - 5.11.79.255
```

7.3.52 reboot

Перезагрузка системы.

Синтаксис
```
reboot [at <время> | cancel | now]
```

Режим интерфейса
Эксплуатационный режим.

Параметры
время

Время, на которое запланирована перезагрузка системы. Дата, и при необходимости время, устанавливаются непосредственно в одном из следующих форматов:

- ЧЧ:ММ
- ДД.ММ.ГГГГ
- ЧЧ:ММ ДД.ММ.ГГГГ
- midnight
- noon
- 'now + N <единиц>'

Обратите внимание, что в поле часов (чч) используется 24-часовая запись (например, 3:00 пополудни будет представлено числом 15 в поле часов).

Обратите также внимание, что единицы могут принимать значение **minutes**, **hours**, **days**, **weeks**, **months** или **years**.

cancel

Отмена перезагрузки, ранее поставленной в расписание.

now

Перезагрузка системы без подтверждения мгновенно.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для перезагрузки системы.

Перед перезагрузкой системы всем вошедшим в систему пользователям рассылается вещательное сообщение, предупреждающее их о перезагрузке.

В том случае если указывается момент времени меньше текущего без указания даты, перезагрузка системы планируется в указанный момент времени следующего дня. В том случае если указывается дата без указания времени, перезагрузка планируется на 00 часов 00 минут указанного дня.

Примеры

В примере выполняется перезагрузка системы.

Пример 42– Перезагрузка системы

```
admin@edge:~$ reboot
Приступить к перезагрузке? [подтвердите (y/n)]y

Broadcast message from root (ttyS0) (Tue Oct 30 16:44:28 2018):

The system is going down for reboot NOW!
```

В примере выполняется перезагрузка системы в указанный день.

Пример 43– Перезагрузка системы в указанный день

```
admin@edge:~$ reboot at 31.10.2018
Планируется перезагрузка на Wed Oct 31 00:00:00 2018
Запланировать перезагрузку? [подтвердите (y/n)]y

Запланирована перезагрузка на Wed Oct 31 00:00:00 2018
```

7.3.53 show arp <интерфейс>

Отображение кэша ARP системы.

Синтаксис
```
show arp <интерфейс>
```

Режим интерфейса
Эксплуатационный режим.

Параметры
интерфейс

Отображение сведений ARP для указанного интерфейса.

Значение по умолчанию
Отсутствует.

Указания по использованию
Эта команда используется для отображения кэша ARP системы. В таблице показаны возможные состояния ARP.

Таблица 16 – Состояния ARP

Значение	Описание
incomplete (неполное)	В настоящий момент на этом соседнем элементе выполняется разрешение адреса.
reachable (достижимое)	Признак достижимости данного соседнего элемента. Получено положительное подтверждение, и путь к данному соседнему элементу работоспособен.
stale (просроченное)	С момента, когда от этого соседнего элемента было получено подтверждение достижимости, прошло времени больше, чем настроенное затраченное время.
delay (задержка)	С момента, когда от этого соседнего элемента было получено подтверждение достижимости, прошло времени больше, чем настроенное затраченное время. Это состояние позволяет протоколу TCP подтвердить соседний элемент. Если это не так, после истечения следующего интервала задержки следует отправить запрос для проверки.
probe (проверка)	Отправлен запрос на предложение, и система ждет ответа от этого соседнего элемента.
failed (сбой)	Сбой обнаружения состояния достижимости соседнего элемента.
noarp (без arp)	Это псевдосостояние, означающее, что для этого элемента соседа ARP не используется.
permanent (постоянное)	Это псевдосостояние, означающее, что данный элемент не может быть вычищен из кэша.
none (отсутствует)	Отсутствует определенное состояние.

Примеры
В примере показан кэш ARP системы edge.

Пример 44– Отображение кэша ARP

```
admin@edge:~$ show arp
? (192.168.10.1) at 00:90:0b:1f:45:15 [ether]  on eth2
? (192.168.10.254) at 00:90:0b:6e:ff:ac [ether]  on eth2
admin@edge:~$
```

7.3.54 show dhcp leases

Отображение сведений о текущих выданных настроенным сервером DHCP адресах.

Синтаксис
```
show dhcp leases
```

Режим интерфейса
Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для просмотра выданных адресов настроенным сервером DHCP в системе.

Примеры

В примере показаны сведения о выданных адресах сервером DHCP в системе Edge1.

Пример 45– Отображение сведений о выданных адресах сервером DHCP

```
admin@Edge1:~$ show dhcp leases
 IP address       Hardware Address    Lease expiration          Subnet
Client Name
 ----------       ----------------    ----------------          ---------
-----------
 192.168.10.186   00:90:0b:73:b2:a5   Thu Feb 27 09:14:46 2020
192.168.10.0/24  Edge2

admin@Edge1:~$
```

7.3.55 show dhcp client leases

Отображение сведений о текущих полученных клиентом DHCP адресах.

Синтаксис

```
show dhcp client leases [interface <интерфейс>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

интерфейс

Просмотр полученных адресов на указанном интерфейсе

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для просмотра полученных адресов настроенным сервером DHCP в системе.

Примеры

В примере показаны сведения о полученных адресах клиентом DHCP в системе Edge2.

Пример 46– Отображение сведений о полученных адресах клиентом DHCP

```
admin@Edge2:~$ show dhcp client leases
interface  : eth1
ip address : 192.168.10.186     [Active]
subnet mask: 255.255.255.0
router     : 192.168.10.254
dhcp server: 192.168.10.254
lease time : 86400
last update: Ср фев 26 12:21:34 MSK 2020
```

```
admin@Edge2:~$
```

7.3.56 show disk <диск> format

Отображение сведений об указанном дисковом устройстве.

Синтаксис

```
show disk <диск> format
```

Режим интерфейса

Эксплуатационный режим.

Параметры

диск

Позволяет указать интересующий диск в системе.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для просмотра сведений о дисковом устройстве в системе.

Примеры

В примере показаны сведения о дисковом устройстве sda в системе edge.

Пример 47– Отображение сведений о дисковом устройстве sda

```
admin@edge:~$ show disk sda format

Disk /dev/sda: 21.4 GB, 21474836480 bytes
16 heads, 63 sectors/track, 41610 cylinders
Units = cylinders of 1008 * 512 = 516096 bytes

   Device Boot      Start         End      Blocks  Id System
/dev/sda1               1           7        3071+ ee EFI GPT
Partition 1 does not end on cylinder boundary
/dev/sda2               7        1022      512000  83 Linux
Partition 2 does not end on cylinder boundary
/dev/sda3            1022        2242      614400  83 Linux
Partition 3 does not end on cylinder boundary
/dev/sda4            2242       41611    19842031+ 83 Linux
Partition 4 does not end on cylinder boundary
admin@edge:~$
```

7.3.57 show files <каталог>

Отображение сведений о файлах.

Синтаксис

```
show files <каталог>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

каталог

Обязательный. Абсолютный или относительный путь к файлам, сведения о которых нужно показать. Обратите внимание, что сведения о самом корневом каталоге ("/") показать нельзя.

ПРИМЕЧАНИЕ Обратите внимание, что сведения о самом корневом каталоге ("/") показать нельзя.

Значение по умолчанию
Отсутствует.

Указания по использованию
Эта команда используется для отображения сведений о файлах в указанном каталоге.

Примеры
В примере показаны сведения о файлах в каталоге /etc/config в системе edge.

Пример 48– Отображение сведений о файлах

```
admin@edge:~$ show files /etc/config
drwxrwxr-x    2 root     root         4.0K Dec  3 02:05 active
-rw-rw----    1 root     vyattacf     2.4K Dec  7 09:43 config.boot
-rw-rw-r--    1 root     vyattacf     2.4K Dec  7 09:43 config.boot~
admin@edge:~$
```

7.3.58 show hardware cpu

Отображение сведений о процессоре системы.

Синтаксис
```
show hardware cpu [summary]
```

Режим интерфейса
Эксплуатационный режим.

Параметры
summary

Показать краткие сведения о центральном процессоре системы.

Значение по умолчанию
Отсутствует.

Указания по использованию
Эта команда используется для просмотра сведений о процессоре или процессорах в аппаратной платформе системы.

Примеры
В примере выводятся сведения о ЦП в системе edge.

Пример 49– Вывод сведений о ЦП

```
processor       : 0
vendor_id       : GenuineIntel
cpu family      : 6
model           : 55
model name      : Intel(R) Atom(TM) CPU  E3825  @ 1.33GHz
stepping        : 9
microcode       : 0x90a
cpu MHz         : 802.097
```

```
cache size      : 512 KB
physical id     : 0
siblings        : 2
core id         : 0
cpu cores       : 2
apicid          : 0
initial apicid  : 0
fpu             : yes
fpu_exception   : yes
cpuid level     : 11
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx
rdtscp lm constant_tsc arch_perfmon pebs bts rep_good nopl xtopology
tsc_reliable nonstop_tsc cpuid aperfmperf tsc_known_freq pni pclmulqdq dtes64
monitor ds_cpl vmx est tm2 ssse3 cx16 xtpr pdcm sse4_1 sse4_2 movbe popcnt
tsc_deadline_timer rdrand lahf_lm 3dnowprefetch epb pti ibrs ibpb stibp
tpr_shadow vnmi flexpriority ept vpid tsc_adjust smep erms dtherm arat
bugs            : cpu_meltdown spectre_v1 spectre_v2
bogomips        : 2666.00
clflush size    : 64
cache_alignment : 64
address sizes   : 36 bits physical, 48 bits virtual
power management:

processor       : 1
vendor_id       : GenuineIntel
cpu family      : 6
model           : 55
model name      : Intel(R) Atom(TM) CPU  E3825  @ 1.33GHz
stepping        : 9
microcode       : 0x90a
cpu MHz         : 533.200
cache size      : 512 KB
physical id     : 0
siblings        : 2
core id         : 2
cpu cores       : 2
apicid          : 4
initial apicid  : 4
fpu             : yes
fpu_exception   : yes
cpuid level     : 11
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx
rdtscp lm constant_tsc arch_perfmon pebs bts rep_good nopl xtopology
tsc_reliable nonstop_tsc cpuid aperfmperf tsc_known_freq pni pclmulqdq dtes64
monitor ds_cpl vmx est tm2 ssse3 cx16 xtpr pdcm sse4_1 sse4_2 movbe popcnt
tsc_deadline_timer rdrand lahf_lm 3dnowprefetch epb pti ibrs ibpb stibp
tpr_shadow vnmi flexpriority ept vpid tsc_adjust smep erms dtherm arat
bugs            : cpu_meltdown spectre_v1 spectre_v2
bogomips        : 2666.00
clflush size    : 64
cache_alignment : 64
address sizes   : 36 bits physical, 48 bits virtual
power management:
```

7.3.59 show hardware dmi

Отображение сведений об интерфейсе DMI системы.

Синтаксис

```
show hardware dmi
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для просмотра сведений об интерфейсе управления рабочей средой (DMI) системы.

Примеры

В примере выводятся сведения об интерфейсе DMI в системе edge.

Пример 50– Вывод сведений об интерфейсе DMI

```
admin@edge:~$ show hardware dmi
bios_date: 31.01.2020 06:37:51
bios_vendor: NumaTech
bios_version: 1.00.000
board_asset_tag:
board_name: NCA-1010B
board_vendor: LANNER
board_version: 2.0
chassis_asset_tag: Default string
chassis_type: 3
chassis_vendor: Default string
chassis_version: Default string
product_family:
product_name: NumaEdge-10
product_sku:
product_version: 1.0
sys_vendor: NumaTech
admin@edge:~$
```

7.3.60 show hardware mem

Отображение сведений о памяти системы.

Синтаксис

```
show hardware mem
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для просмотра сведений о памяти системы.

Примеры

В примере выводятся сведения о памяти в системе edge.

Пример 51– Вывод сведений о памяти

```
admin@edge:~$ show hardware mem
MemTotal:        3855204 kB
MemFree:         3651520 kB
MemAvailable:    3496200 kB
Buffers:           36976 kB
Cached:            50304 kB
SwapCached:            0 kB
Active:            91436 kB
Inactive:          22392 kB
Active(anon):      26744 kB
Inactive(anon):      308 kB
Active(file):      64692 kB
Inactive(file):    22084 kB
Unevictable:           0 kB
Mlocked:               0 kB
SwapTotal:             0 kB
SwapFree:              0 kB
Dirty:                84 kB
Writeback:             0 kB
AnonPages:         26512 kB
Mapped:            15364 kB
Shmem:               504 kB
Slab:              61288 kB
SReclaimable:      45444 kB
SUnreclaim:        16024 kB
KernelStack:        1588 kB
PageTables:         2852 kB
NFS_Unstable:          0 kB
Bounce:                0 kB
WritebackTmp:          0 kB
CommitLimit:     1927600 kB
Committed_AS:      83924 kB
VmallocTotal:   34359738367 kB
VmallocUsed:           0 kB
VmallocChunk:          0 kB
Percpu:              592 kB
HardwareCorrupted:     0 kB
AnonHugePages:         0 kB
ShmemHugePages:        0 kB
ShmemPmdMapped:        0 kB
DirectMap4k:       52144 kB
DirectMap2M:     3942400 kB
DirectMap1G:           0 kB
admin@edge:~$
```

7.3.61 show hardware pci

Отображение сведений о шине PCI системы.

Синтаксис

```
show hardware pci [detailed]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

detailed

Вывод подробных сведений о шине PCI.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для просмотра сведений о шине PCI. Шина PCI обеспечивает связь между периферийными компонентами системы и процессором.

Примеры

В примере выводятся сведения о шине PCI в системе edge.

Пример 52– Вывод сведений о шине PCI

```
admin@edge:~$ show  hardware pci
00:00.0 Host bridge: Intel Corporation ValleyView SSA-CUnit (rev 11)
00:02.0 VGA compatible controller: Intel Corporation ValleyView Gen7 (rev 11)
00:13.0 SATA controller: Intel Corporation ValleyView 6-Port SATA AHCI
Controller (rev 11)
00:14.0 USB controller: Intel Corporation ValleyView USB xHCI Host Controller
(rev 11)
00:1a.0 Encryption controller: Intel Corporation ValleyView SEC (rev 11)
00:1b.0 Audio device: Intel Corporation ValleyView High Definition Audio
Controller (rev 11)
00:1c.0 PCI bridge: Intel Corporation ValleyView PCI Express Root Port (rev
11)
00:1c.1 PCI bridge: Intel Corporation ValleyView PCI Express Root Port (rev
11)
00:1c.2 PCI bridge: Intel Corporation ValleyView PCI Express Root Port (rev
11)
00:1c.3 PCI bridge: Intel Corporation ValleyView PCI Express Root Port (rev
11)
00:1f.0 ISA bridge: Intel Corporation ValleyView Power Control Unit (rev 11)
00:1f.3 SMBus: Intel Corporation ValleyView SMBus Controller (rev 11)
02:00.0 Ethernet controller: Intel Corporation I211 Gigabit Network Connection
(rev 03)
03:00.0 Ethernet controller: Intel Corporation I211 Gigabit Network Connection
(rev 03)
04:00.0 Ethernet controller: Intel Corporation I211 Gigabit Network Connection
(rev 03)
admin@edge:~$
```

7.3.62 show history

Отображение журнала выполнения команд.

Синтаксис

show history [<число> | brief]

Режим интерфейса

Эксплуатационный режим.

Параметры

число

Количество последних команд, которые будут отображены.

brief

Отображение последних 20 команд.

Значение по умолчанию

Отображается весь журнал команд.

Указания по использованию

Эта команда используется для просмотра журнала выполнения команд в системе. Если вывод занимает более чем одну страницу, появляется запрос с двоеточием (":"). Для отображения следующего экрана нажмите клавишу <Пробел>, для отображения следующей строки клавишу <Enter>, для остановки вывода клавишу "q".

Примеры

В примере выводится журнал выполнения команд в системе edge.

Пример 53– Отображение журнала команд

```
admin@edge:~$ show history
 1  2018-10-30T15:23:37+0300 configure
  2  2018-10-30T15:23:42+0300 commit
  3  2018-10-30T15:23:44+0300 exit
  4  2018-10-30T15:23:51+0300 show version
  5  2018-10-30T15:23:55+0300 configure
  6  2018-10-30T15:23:58+0300 exit
  7  2018-10-30T15:24:15+0300 show hardware pci
  8  2018-10-30T15:24:22+0300 configure
  9  2018-10-30T15:24:50+0300 set interfaces ethernet eth3 address dhcp
 10  2018-10-30T15:25:17+0300 show
 11  2018-10-30T15:25:26+0300 show service ssh
 12  2018-10-30T15:25:31+0300 exit
 13  2018-10-30T15:25:44+0300 show arp
 14  2018-10-30T15:25:50+0300 show history
admin@edge:~$
```

7.3.63 show host

Отображение сведений об узлах, достижимых для системы.

Синтаксис

```
show host [lookup [<имя_узла> | <ipv4-адрес> | <ipv6-адрес>] | name | os]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

lookup *имя_узла*

Для узла с указанным именем выводятся каноническое имя и IP-адрес, а также все настроенные псевдонимы, зарегистрированные на сервере имен.

lookup *ipv4-адрес*

Для узла с указанным IP-адресом выводятся каноническое имя и IP-адрес, а также все настроенные псевдонимы, зарегистрированные на сервере имен.

lookup *ipv6-адрес*

Для узла с указанным IP-адресом выводятся каноническое имя и IP-адрес, а также все настроенные псевдонимы, зарегистрированные на сервере имен.

name

Вывод имени, настроенного для данной системы.

os

Вывод подробностей об ОС системы.

Значение по умолчанию
Отсутствует.

Указания по использованию
Эта команда используется для просмотра сведений, настроенных для узла.

Примеры
В примере выводятся сведения об узле для Edge2.

Пример 54 – Поиск узлов в сети

```
admin@Edge1:~$ show host lookup Edge2
Server: 127.0.0.1
Address 1: 127.0.0.1 localhost.localdomain

Name: Edge2
Address 1: 192.168.20.254 Edge2
admin@Edge1:~$
```

В примере выводится имя, настроенное для Edge1.

Пример 55– Вывод имен узлов в сети

```
admin@Edge1:~$ show host name
Edge1
admin@Edge1:~$
```

В примере выводятся информация об операционной системе узла Edge1.

Пример 56– Вывод сведений об операционной системе

```
admin@Edge1:~$ show host os
Linux Edge1 4.19.11 #numa-edge SMP 2019-01-01 12:00:00 +0400 x86_64 GNU/Linux
admin@Edge1:~$
```

7.3.64 show interfaces

Отображение сведений о системных интерфейсах.

Синтаксис
```
show interfaces [counters | <интерфейс> [detail]| detail | system [enabled]]
```

Режим интерфейса
Эксплуатационный режим.

Параметры
counters

Отображение значения счетчиков переданных/принятых пакетов и переданных/принятых байт для всех интерфейсов, доступных в системе.

интерфейс

Вывод сведений только об интерфейсах указанного типа.

detail

Отображение подробных сведений об интерфейсах.

system

Отображение всех физических интерфейсов, имеющихся в системе.

enabled

Вывод только включенных интерфейсов, известных ядру операционной системы.

Значение по умолчанию

Отображение сведений для всех интерфейсов, настроенных в системе.

Указания по использованию

Эта команда используется для просмотра сведений о настройке и состоянии работоспособности для интерфейсов и виртуальных интерфейсов.

При использовании без параметров команда отображает сведения обо всех интерфейсах, настроенных в системе. Конкретные сведения можно вывести с помощью других версий этой команды:

Для вывода всех физических интерфейсов, известных ядру операционной системы, используется параметр system. Этот вариант команды отличается от других ее вариантов: в других вариантах выводятся интерфейсы, настроенные в системе, в то время как при использовании параметра system выводятся все физические интерфейсы, имеющиеся в системе (то есть физические интерфейсы, известные ядру системы).

ПРИМЕЧАНИЕ Подробно команды отображения сведений об интерфейсах рассмотрены в разделе Настройка интерфейсов

Список наличествующих физических интерфейсов определяет, какие интерфейсы можно будет настроить и просмотреть, поскольку физически не существующий в системе интерфейс нельзя настроить или просмотреть.

Примеры

В примере выведен первый экран результата работы команды show interfaces system enabled.

Пример 57– Отображение сведений об интерфейсах

```
admin@edge:~$ show interfaces system enabled
eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group
default qlen 1000
    link/ether 00:90:0b:a3:44:ca brd ff:ff:ff:ff:ff:ff
    inet 192.168.110.2/24 brd 192.168.110.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::290:bff:fea3:44ca/64 scope link
       valid_lft forever preferred_lft forever
    RX: bytes  packets  errors  dropped overrun mcast
    1023016    14221    0       0       0       20
    TX: bytes  packets  errors  dropped carrier collsns
    1235089    6052     0       0       0       0

    RX:  bytes    packets     errors    dropped    overrun      mcast
       1023016      14221          0          0          0         20
    TX:  bytes    packets     errors    dropped    carrier collisions
       1235089       6052          0          0          0          0

ethm: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group
default qlen 1000
    link/ether 00:90:0b:a3:44:c9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.200.1/24 scope global ethm
       valid_lft forever preferred_lft forever
    RX: bytes  packets  errors  dropped overrun mcast
    0          0        0       0       0       0
    TX: bytes  packets  errors  dropped carrier collsns
    0          0        0       0       0       0

    RX:  bytes    packets     errors    dropped    overrun      mcast
             0          0          0          0          0          0
    TX:  bytes    packets     errors    dropped    carrier collisions
             0          0          0          0          0          0
```

```
lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
    RX: bytes  packets  errors  dropped overrun mcast
    16072      232      0       0       0       0
    TX: bytes  packets  errors  dropped carrier collsns
    16072      232      0       0       0       0

    RX:  bytes    packets     errors    dropped    overrun      mcast
         16072        232          0          0          0          0
    TX:  bytes    packets     errors    dropped    carrier collisions
         16072        232          0          0          0          0

admin@edge:~$
```

7.3.65 show interfaces stat <интерфейс>

Отображение статистики использования интерфейса.

Синтаксис

```
show interfaces stat <интерфейс> [<from <date_start> [to <date_end> [step
<step_rate>]]]
```

Режим интерфейса

Эксплуатационный режим

Параметры

интерфейс

Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже в разделе "Указания по использованию".

from *date_start*

Указание начала временного отрезка вывода статистики. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже в разделе "Указания по использованию".

to *date_end*

Указание конца временного отрезка вывода статистики. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже в разделе "Указания по использованию".

step *step_rate*

Указание величины шага для отображения статистики. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже в разделе "Указания по использованию".

ПРИМЕЧАНИЕ При использовании больших временных отрезков, указание шага будет иметь приблизительные значения, в связи с усреднением хранящейся статистики. Например, для суточного интервала рекомендуется использовать шаг не менее 1 часа.

Значение по умолчанию

Отображается информация за последний час с интервалом в 5 минут.

Указания по использованию

Эта команда используется для просмотра сведений о нагрузке на интерфейс за определенный промежуток времени.

В приведенной ниже таблице показан синтаксис и параметры поддерживаемых типов интерфейсов.

Таблица 17 – Синтаксис и параметры поддерживаемых типов интерфейсов

Тип интерфейса	**Синтаксис**
Агрегирование каналов	bondx
Виртуальный интерфейс агрегированных каналов	bondx.идентификатор_vlan
Сетевой мост	brx
Ethernet	ethx
Ethernet PPPoE	pppoe1
Виртуальный интерфейс Ethernet	ethx.идентификатор_vlan
Интерфейс заглушки	lo
Многоканальная связь	mlx
OpenVPN	vtunx
Псевдо-Ethernet	pethx
Последовательный PPP	wanx
Туннель	tunx

Для указания времени суток используется формат ввода вида HH:MM. Также возможно использование суффиксов am и pm или указание особых временных значений дня, таких как noon (12:00) и midnight (00:00).

День может быть указан как «Название месяца» «День месяца» и двухзначное или четырехзначное значение года (например, March 8 2018). В качестве альтернативы можно использовать название дня недели (например, «Monday») или одно из слов: yesterday (пер. вчера), today (пер. сегодня), tomorrow (пер. завтра). День также можно указать как полную дату в числовом формате вида DD.MM.[YY]YY

Таблица 18 – Значения дней недели

Значение	**Описание**
Monday	Понедельник
Tuesday	Вторник
Wednesday	Среда
Thursday	Четверг
Friday	Пятница
Saturday	Суббота
Sunday	Воскресенье

В таблице показаны возможные значения месяцев.

Таблица 19– Значения месяцев

Значение	**Описание**
January	Январь
February	Февраль
March	Март
April	Апрель
May	Май
June	Июнь
July	Июль
August	Август
September	Сентябрь
October	Октябрь
November	Ноябрь
December	Декабрь

Название месяцев и дней недели можно использовать в их естественно сокращенной форме (например, December – dec, Monday – mon).

При использовании характеристики временного смещения, к моменту отсчета времени добавляется (или вычитается из него) определенный временной интервал. Для этого используется знак («+» или «-») и временной интервал. Единицы измерения временных интервалов указываются в виде суффиксов, представленных в таблице.

Таблица 20 – Единицы измерения временных интервалов

Суффикс	**Описание**
min	Минута
h	Час
d	День
w	Неделя
month	Месяц
y	Год

Несколько единиц измерения могут быть объединены (например, -5mon1w2d) или просуммированы (например, -5h-45min = -6h+15min = -7h +1h30min -15min).

В приведенной ниже таблице показаны примеры указания временных значений.

Таблица 21 – Примеры указания временного значения

Значение времени	**Описание**
14:15	15 минут третьего, сегодняшнего дня
23:59 31.12.2018	Одна минута до 2018-го года
Oct 12	12 октября текущего года
March 8 2019	8-ое марта 2019-ого года
Sunday	Последнее воскресенье
now	В данный момент
yesterday	Вчера
today	Сегодня
20181031	31-ое октября 2018-ого года
now-1d или -1d	Один день назад
-1w+1h30min	Неделю назад, плюс полтора часа вперед
noon yesterday -3hours	3 часа до полудня вчерашнего дня

Примеры

В примере ниже представлен вывод нагрузки на сетевой интерфейс eth1 за последний час, с интервалом вывода в 5 минут.

Пример 58– Вывод нагрузки на сетевой интерфейс

```
admin@edge:~$ show interfaces stat eth1
       Time       |   RX total    |  RX average  |   TX total    |  TX average
------------------+---------------+--------------+---------------+--------------
 2019-04-26 15:43 |   0.0  bytes  |   0.0  bit/s |   0.0  bytes  |   0.0  bit/s
 2019-04-26 15:48 |   0.0  bytes  |   0.0  bit/s |   0.0  bytes  |   0.0  bit/s
 2019-04-26 15:53 |   0.0  bytes  |   0.0  bit/s |   0.0  bytes  |   0.0  bit/s
 2019-04-26 15:58 |   0.0  bytes  |   0.0  bit/s |   0.0  bytes  |   0.0  bit/s
 2019-04-26 16:03 |   0.0  bytes  |   0.0  bit/s |   0.0  bytes  |   0.0  bit/s
 2019-04-26 16:08 |   0.0  bytes  |   0.0  bit/s |   0.0  bytes  |   0.0  bit/s
 2019-04-26 16:13 |   0.0  bytes  |   0.0  bit/s |   0.0  bytes  |   0.0  bit/s
 2019-04-26 16:18 |   0.0  bytes  |   0.0  bit/s |   0.0  bytes  |   0.0  bit/s
 2019-04-26 16:23 |   0.0  bytes  |   0.0  bit/s |   0.0  bytes  |   0.0  bit/s
 2019-04-26 16:28 |   0.0  bytes  |   0.0  bit/s |   0.0  bytes  |   0.0  bit/s
 2019-04-26 16:33 |   0.0  bytes  |   0.0  bit/s |   0.0  bytes  |   0.0  bit/s
 2019-04-26 16:38 | 136.6 Kbytes  |   3.6 Kbit/s |   4.8 Kbytes  | 129.0  bit/s
 2019-04-26 16:43 |   0.0  bytes  |   0.0  bit/s |   0.0  bytes  |   0.0  bit/s
```

В примере ниже представлен вывод нагрузки на сетевом интерфейсе eth1 за последние 7 минут.

Пример 59– Вывод нагрузки

```
admin@edge:~$ show interfaces stat eth1 from -7min
       Time        |   RX total    |  RX average  |   TX total    |  TX average
-------------------+---------------+--------------+---------------+--------------
 2019-04-26 16:57 |  21.4 Kbytes | 569.6  bit/s |   0.0  bytes |   0.0  bit/s
 2019-04-26 17:02 |  23.7 Kbytes | 631.5  bit/s |   0.0  bytes |   0.0  bit/s
```

В примере ниже представлен вывод нагрузки на сетевом интерфейсе eth1 за временной промежуток начавшийся 7 минут назад и закончившийся минуту назад, с интервалом вывода в 5 минут.

Пример 60– Вывод нагрузки за временной промежуток

```
admin@edge:~$ show interfaces stat eth1 from -7min to -1min
       Time        |   RX total    |  RX average  |   TX total    |  TX average
-------------------+---------------+--------------+---------------+--------------
 2019-04-26 17:01 |  22.5 Kbytes | 600.1  bit/s |  20.7 Kbytes | 552.3  bit/s
 2019-04-26 17:06 |  22.5 Kbytes | 599.0  bit/s |   0.0  bytes |   0.0  bit/s
```

В примере ниже представлен вывод нагрузки на сетевом интерфейсе eth1 за последние 4 минут с интервалом вывода в 1 минуту.

Пример 61– Вывод нагрузки

```
admin@edge:~$ show interfaces stat eth1 from -4min to now step 1min
       Time        |   RX total    |  RX average  |   TX total    |  TX average
-------------------+---------------+--------------+---------------+--------------
 2019-04-26 17:05 |   7.2 Kbytes | 963.2  bit/s |  20.7 Kbytes |   2.8 Kbit/s
 2019-04-26 17:06 |   1.2 Kbytes | 166.0  bit/s | 351.1  bytes |  46.8  bit/s
 2019-04-26 17:07 |   8.5 Kbytes |   1.1 Kbit/s |   0.0  bytes |   0.0  bit/s
 2019-04-26 17:08 |   3.2 Kbytes | 422.0  bit/s |   0.0  bytes |   0.0  bit/s
 2019-04-26 17:09 |   5.5 Kbytes | 739.2  bit/s |   4.0 Kbytes | 529.7  bit/s
 2019-04-26 17:10 |   0.0  bytes |   0.0  bit/s |   0.0  bytes |   0.0  bit/s
```

7.3.66 show reboot

Отображение даты и времени следующей запланированной перезагрузки.

Синтаксис

```
show reboot
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для просмотра даты и времени следующей запланированной перезагрузки. Время следующей запланированной перезагрузки задается командой **reboot at**.

Примеры

В примере выводятся дата и время следующей запланированной перезагрузки.

Пример 62– Вывод следующей запланированной перезагрузки

```
admin@edge:~$ show reboot
Запланирована перезагрузка на Wed Oct 31 15:30:00 2018
admin@edge:~$
```

В примере выводится пустой список запланированных перезагрузок.

Пример 63– Вывод пустого списка запланированных перезагрузок

```
admin@edge:~$ show reboot
Не обнаружено запланированных перезагрузок
admin@edge:~$
```

7.3.67 show serial

Отображение сведений о серийном номере изделия.

Синтаксис

show serial

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для вывода серийного номера изделия.

Примеры

В примере выведен первый экран результатов работы команды show serial.

Пример 64– Отображение сведений о серийном номере

```
admin@edge:~$ show serial
00001.1
```

7.3.68 show shutdown

Отображение даты и времени следующего запланированного выключения.

Синтаксис

`show shutdown`

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для просмотра даты и времени следующего запланированного выключения. Время следующего запланированного выключения задается командой shutdown at.

Примеры

В примере ниже выводятся дата и время следующей запланированной перезагрузки системы edge.

Пример 65– Вывод следующей запланированной перезагрузки

```
admin@Edge1:~$ show shutdown
Shutdown pending at 15:45
admin@Edge1:~$
```

В примере ниже выводится пустой список запланированных перезагрузок.

Пример 66– Вывод пустого списка запланированных перезагрузок

```
admin@edge:~$ show shutdown
No shutdown pending
admin@edge:~$
```

7.3.69 show snmp mib ifmib

Отображение сведения об интерфейсах из базы управляющей информации протокола SNMP.

Синтаксис

```
show snmp mib ifmib <параметр>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

параметр

Вывести информацию об указанном параметре для всех сконфигурированных интерфейсов в системе. Для выбора доступны следующие параметры: ifAlias, ifIndex, ifDescr.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения сведений об интерфейсах из базы управляющей информации протокола SNMP. По умолчанию без дополнительных параметров выводится вся имеющаяся информация о доступных параметрах.

Примеры

В примере ниже приведен результат выполнения команды show snmp mib ifmib системы edge.

Пример 67– Отображение сведений об интерфейсах из базы управляющей информации протокола SNMP.

```
admin@edge:~$ show snmp mib ifmib
br0: ifIndex = 6
eth1: ifIndex = 3
      ifDescr = Intel Corporation 82540EM Gigabit Ethernet Controller
eth2: ifIndex = 4
      ifDescr = Intel Corporation 82540EM Gigabit Ethernet Controller
eth3: ifIndex = 5
      ifDescr = Intel Corporation 82540EM Gigabit Ethernet Controller
ethm: ifIndex = 2
```

```
      ifDescr = Intel Corporation 82540EM Gigabit Ethernet Controller
lo: ifIndex = 1
admin@edge:~$
```

В примере ниже приведен результат выполнения команды show snmp mib ifmib с параметром ifAlias.

Пример 68– Отображение сведений о параметре ifAlias для интерфейсов системы из базы управляющей информации протокола SNMP

```
admin@Edge1:~$ show snmp mib ifmib ifAlias
br0: ifAlias = br0
eth1: ifAlias = eth1
eth2: ifAlias = eth2
eth3: ifAlias = eth3
ethm: ifAlias = ethm
lo: ifAlias = lo
admin@Edge1:~$
```

7.3.70 show system boot-messages

Отображение сообщений, созданных ядром при загрузке.

Синтаксис

```
show system boot-messages
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для вывода сообщений во время загрузки, созданных ядром.

Примеры

В примере выведен первый экран результатов работы команды show system boot-messages.

Пример 69– Отображение сообщений при загрузке

```
[    0.000000] Linux version 4.19.11 (robo@numatech.ru) (gcc version 4.9.2
(GCC)) #numa-edge SMP 2018-10-30 12:00:00 +0400
[    0.000000] Command line: console=tty0 console=ttyS0,115200 quiet
[    0.000000] KERNEL supported cpus:
[    0.000000]   Intel GenuineIntel
[    0.000000]   AMD AuthenticAMD
[    0.000000] x86/fpu: x87 FPU will use FXSAVE
[    0.000000] BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009cbff] usable
[    0.000000] BIOS-e820: [mem 0x000000000009cc00-0x000000000009ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000000e0000-0x00000000000fffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000000100000-0x000000001efffffe] usable
[    0.000000] BIOS-e820: [mem 0x000000001f000000-0x000000001f0fffff] reserved
[    0.000000] BIOS-e820: [mem 0x000000001f100000-0x000000001fffffff] usable
[    0.000000] BIOS-e820: [mem 0x0000000020000000-0x00000000200fffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000020100000-0x00000000adffffff] usable
[    0.000000] BIOS-e820: [mem 0x00000000ae000000-0x00000000b001ffff] reserved
```

```
[    0.000000] BIOS-e820: [mem 0x00000000b0020000-0x00000000b0ceafff] usable
[    0.000000] BIOS-e820: [mem 0x00000000b0ceb000-0x00000000b0d34fff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000b0d35000-0x00000000b0d7efff] ACPI NVS
[    0.000000] BIOS-e820: [mem 0x00000000b0d7f000-0x00000000b0d85fff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000b0d86000-0x00000000b0d8dfff] ACPI NVS
...
```

7.3.71 show system connections

Отображение активных сетевых подключений в системе.

Синтаксис

```
show system connections [tcp [numeric] | udp [numeric]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

tcp

Показывает информацию о подключениях по протоколу TCP.

udp

Показывает информацию о подключениях по протоколу UDP.

numeric

Показывает информацию о подключениях по протоколу TCP или UDP без разрешения имён.

Значение по умолчанию

При отсутствии дополнительных параметров команда используется для вывода всех активных сетевых подключений.

Указания по использованию

Эта команда используется для вывода списка сетевых подключений, активных в сети в настоящее время.

Примеры

В примере выведен первый экран результатов работы команды show system connections.

Пример 70– Отображение активных подключений

```
admin@edge:~$ show system connections
Netid  State      Recv-Q Send-Q Local Address:Port                 Peer
Address:Port
u_str  ESTAB      0      0      /dev/log 4020                 * 4019
u_str  ESTAB      0      0       * 4019                  * 4020
u_str  ESTAB      0      0       * 5222                  * 5223
u_str  ESTAB      0      0      /dev/log 13838                * 13835
u_str  ESTAB      0      0       * 12152                 * 12169
u_str  ESTAB      0      0       * 12267                 * 12315
u_str  ESTAB      0      0       * 3901                  * 3902
u_str  ESTAB      0      0      /dev/log 3710                 * 3709
udp    ESTAB      0      0      10.150.150.155:54505
88.147.254.230:ntp
```

7.3.72 show system kernel-messages

Отображение сообщений в кольцевом буфере ядра.

Синтаксис

```
show system kernel-messages
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для вывода сообщений, в настоящий момент находящихся в кольцевом буфере ядра.

Примеры

В примере выведен первый экран результатов работы команды show system kernel-messages.

Пример 71– Отображение сообщений ядра

```
admin@edge:~$ show system kernel-messages
[    0.000000] Linux version 4.19.11 (robo@numatech.ru) (gcc version 4.9.2
(GCC)) #numa-edge SMP 2018-10-30 12:00:00 +0400
[    0.000000] Command line: console=tty0 console=ttyS0,115200 quiet
[    0.000000] KERNEL supported cpus:
[    0.000000]   Intel GenuineIntel
[    0.000000]   AMD AuthenticAMD
[    0.000000] x86/fpu: x87 FPU will use FXSAVE
[    0.000000] BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009cbff] usable
[    0.000000] BIOS-e820: [mem 0x000000000009cc00-0x000000000009ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000000e0000-0x00000000000fffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000000100000-0x000000001efffffe] usable
[    0.000000] BIOS-e820: [mem 0x000000001f000000-0x000000001f0fffff] reserved
[    0.000000] BIOS-e820: [mem 0x000000001f100000-0x000000001fffffff] usable
[    0.000000] BIOS-e820: [mem 0x0000000020000000-0x00000000200fffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000020100000-0x00000000adffffff] usable
[    0.000000] BIOS-e820: [mem 0x00000000ae000000-0x00000000b001ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000b0020000-0x00000000b0ceafff] usable
[    0.000000] BIOS-e820: [mem 0x00000000b0ceb000-0x00000000b0d34fff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000b0d35000-0x00000000b0d7efff] ACPI NVS
[    0.000000] BIOS-e820: [mem 0x00000000b0d7f000-0x00000000b0d85fff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000b0d86000-0x00000000b0d8dfff] ACPI NVS
[    0.000000] BIOS-e820: [mem 0x00000000b0d8e000-0x00000000b1591fff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000b1592000-0x00000000b1592fff] ACPI NVS
[    0.000000] BIOS-e820: [mem 0x00000000b1593000-0x00000000b15a8fff] ACPI
data
[    0.000000] BIOS-e820: [mem 0x00000000b15a9000-0x00000000b15a9fff] ACPI NVS
[    0.000000] BIOS-e820: [mem 0x00000000b15aa000-0x00000000b15aafff] ACPI
data
[    0.000000] BIOS-e820: [mem 0x00000000b15ab000-0x00000000b15dcfff] ACPI NVS
[    0.000000] BIOS-e820: [mem 0x00000000b15dd000-0x00000000b18ecfff] reserved
...
```

7.3.73 show system memory

Отображение использования памяти системой.

Синтаксис

```
show system memory [quagga | detail]
```

Режим интерфейса
Эксплуатационный режим.

Параметры
quagga

Отображение использования памяти подсистемой Quagga.

detail

Отображает детальную информацию об использовании памяти.

Значение по умолчанию
Отсутствует.

Указания по использованию
Эта команда используется для выводит количество памяти, используемое в данный момент системой, и количество свободной памяти.

Примеры
В примере выводятся сведения об использовании памяти в системе edge.

Пример 72– Отображение сведений об использовании памяти

```
admin@edge:~$ show system memory
              total        used        free      shared  buff/cache
available
Mem:          241184       56024       41084         620      144076
176188
Swap:              0           0           0
Total:        241184       56024       41084
```

7.3.74 show system processes

Отображение активных процессов в системе.

Синтаксис
```
show system processes [summary]
```

Режим интерфейса
Эксплуатационный режим.

Параметры
summary

Вывод сводки об использовании системы.

Значение по умолчанию
Вывод списка всех процессов, работающих в системе в настоящее время.

Указания по использованию
Эта команда используется для вывода сведений о процессах, работающих в системе в настоящее время.

Примеры
В примере выведен первый экран результатов работы команды show system processes.

Пример 73– Отображение сведений о процессах

```
admin@edge:~$ show system processes
  PID TTY      STAT   TIME COMMAND
```

```
    1 ?        Ss     0:03 init [5]
    2 ?        S      0:00 [kthreadd]
    3 ?        I<     0:00 [rcu_gp]
    4 ?        I<     0:00 [rcu_par_gp]
    5 ?        I      0:00 [kworker/0:0-rcu]
    6 ?        I<     0:00 [kworker/0:0H-kb]
    8 ?        I<     0:00 [mm_percpu_wq]
    9 ?        S      0:00 [ksoftirqd/0]
   10 ?        I      0:02 [rcu_sched]
   11 ?        I      0:00 [rcu_bh]
   12 ?        S      0:00 [migration/0]
   13 ?        S      0:00 [cpuhp/0]
   14 ?        S      0:00 [cpuhp/1]
   15 ?        S      0:00 [migration/1]
   16 ?        S      0:00 [ksoftirqd/1]
   17 ?        I      0:00 [kworker/1:0-mm_]
   18 ?        I<     0:00 [kworker/1:0H-kb]
   19 ?        S      0:00 [kdevtmpfs]
   20 ?        I<     0:00 [netns]
   21 ?        S      0:00 [kauditd]
   22 ?        I      0:05 [kworker/0:1-eve]
   23 ?        S      0:00 [oom_reaper]
   24 ?        I<     0:00 [writeback]
   25 ?        S      0:00 [kcompactd0]
...
```

7.3.75 show system routing-daemons

Отображение активных служб маршрутизации.

Синтаксис

```
show system routing-daemons
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для вывода списка активных служб маршрутизации.

Примеры

В примере выведены результаты работы команды show system routing-daemons.

Пример 74– Отображение списка активных служб маршрутизации

```
admin@edge:~$ show system routing-daemons
 zebra ripd ripngd ospfd ospf6d bgpd
admin@edge:~$
```

7.3.76 show system sensors

Отображение сведений системных датчиков.

Синтаксис
```
show system sensors
```

Режим интерфейса
Эксплуатационный режим.

Параметры
Отсутствуют.

Значение по умолчанию
Отсутствует.

Указания по использованию
Эта команда используется для вывода информации с имеющихся системных датчиков.

Примеры
В примере выводится информация системных датчиков для системы edge.

Пример 75– Отображение сведений системных датчиков.

```
admin@edge:~$ show system sensors
coretemp-isa-0000
Adapter: ISA adapter
Core 0:       +33.0 C  (high = +98.0 C, crit = +98.0 C)
Core 1:       +33.0 C  (high = +98.0 C, crit = +98.0 C)
Core 2:       +34.0 C  (high = +98.0 C, crit = +98.0 C)
Core 3:       +34.0 C  (high = +98.0 C, crit = +98.0 C)

i350bb-pci-0600
Adapter: PCI adapter
loc1:         +59.0 C  (high = +120.0 C, crit = +110.0 C)

i350bb-pci-0700
Adapter: PCI adapter
loc1:         +60.0 C  (high = +120.0 C, crit = +110.0 C)

admin@edge:~$
```

7.3.77 show system services

Отображение сведений об активных сетевых службах в системе.

Синтаксис
```
show system services [tcp [numeric] | udp [numeric]]
```

Режим интерфейса
Эксплуатационный режим.

Параметры
tcp

Показывает информацию о службах протокола TCP.

udp

Показывает информацию о службах протокола UDP.

numeric

Показывает информацию о службах протокола TCP или UDP без разрешения имён.

Значение по умолчанию

При отсутствии дополнительных параметров команда показывает информацию обо всех активных сетевых службах в системе и портах, которые прослушивают эти службы.

Указания по использованию

Эта команда используется для вывода информации об активных сетевых службах в системе и портах, которые прослушивают эти службы.

Примеры

В примере выводится информация об активных сетевых службах в системе edge.

Пример 76– Отображение сведений о сетевых службах и прослушиваемых ими портов.

```
admin@edge:~$ show system services
Netid  State      Recv-Q Send-Q Local Address:Port                 Peer
Address:Port
udp    UNCONN     0      0      127.0.0.1:domain                *:*
udp    UNCONN     0      0       *:bootps                *:*
udp    UNCONN     0      0         ::1:domain                :::*
tcp    LISTEN     0      3      127.0.0.1:zebra                 *:*
tcp    LISTEN     0      3      127.0.0.1:ripd                  *:*
tcp    LISTEN     0      3      127.0.0.1:ospfd                 *:*
tcp    LISTEN     0      3      127.0.0.1:bgpd                  *:*
tcp    LISTEN     0      128    192.168.200.1:www                   *:*
tcp    LISTEN     0      32     127.0.0.1:domain                *:*
tcp    LISTEN     0      128    192.168.200.1:ssh                   *:*
tcp    LISTEN     0      128    192.168.200.1:https                 *:*
tcp    LISTEN     0      3         ::1:ripngd               :::*
tcp    LISTEN     0      3         ::1:ospf6d               :::*
tcp    LISTEN     0      32        ::1:domain               :::*
admin@edge:~$
```

7.3.78 show system storage

Отображение использования системных файлов системой и доступного места на накопителях.

Синтаксис

```
show system storage
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для вывода количества места на накопителях, используемого в данный момент системой, и количества свободного места.

Примеры

В примере выводятся сведения об использовании места файловой системой на edge.

Пример 77– Отображение сведений о файловой системе и накопителях

```
admin@edge:~$ show system storage
Filesystem                Size      Used Available Use% Mounted on
```

```
/dev/sda2                574.6M    299.9M    244.6M  55% /
/dev/sda3                  6.2G     49.5M      5.8G   1% /cfg
/dev/sda3                  6.2G     49.5M      5.8G   1% /etc
/dev/sda3                  6.2G     49.5M      5.8G   1% /home
/dev/sda3                  6.2G     49.5M      5.8G   1% /var/log
none                       1.8G    328.0K      1.8G   0% /var/volatile
none                       1.8G    176.0K      1.8G   0% /dev
tmpfs                      1.8G         0      1.8G   0% /dev/shm
none                       1.8G    328.0K      1.8G   0%
/var/volatile/run/netns
admin@edge:~$
```

7.3.79 show system uptime

Отображение сведений о длительности работы системы.

Синтаксис

```
show system uptime
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для вывода времени безостановочной работы системы, числа пользователей, в настоящее время вошедших в систему, и средней загрузки системы.

Примеры

В примере выводятся сведения об использовании системы для edge.

Пример 78– Отображение сведений об использовании системы и пользователях

```
admin@edge:~$ show system uptime
 12:01:58 up 37 min,  1 user,  load average: 0.00, 0.00, 0.00
admin@edge:~$
```

7.3.80 show system usb

Отображение сведений о периферийных устройствах, подключенных по шине USB.

Синтаксис

```
show system usb
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для вывода списка устройств, подключенных к шине USB.

Примеры

В примере выводятся сведения об устройствах, подключенных к системе edge по шине USB.

Пример 79– Отображение сведений о периферийных устройствах на шине USB

```
admin@edge:~$ show system usb
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
admin@edge:~$
```

7.3.81 show tech-support

Консолидированный отчет по сведениям о системе.

Синтаксис

```
show tech-support [brief] [save <имя_файла> | save-uncompressed <имя_файла>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

brief

Вывод краткого отчета о системе для обращения в службу поддержки

save

Сохранение сведений о системе для обращения в службу поддержки в виде архива. Для ограничения числа выходных файлов до 10 используется механизм циклического замещения, то есть при создании одиннадцатого файла наиболее старый файл удаляется.

save_uncompressed

Сохранение сведений о системе для обращения в службу поддержки в файл.

имя_файла

Сохранение сведений о поддержке в файл **имя_файла.имя_узла.tech-support.отметка_времени**, где *имя_узла* это имя узла, настроенное для данной машины, а *отметка_времени* это время сохранения файла. Если имени файла предшествует абсолютный путь, файл сохраняется в указанном местоположении. В противном случае файл сохраняется в местоположение относительно пути по умолчанию, которым является каталог */etc/config/support*.

Значение по умолчанию

Сведения отправляются на консоль.

Указания по использованию

Эта команда используется для вывода технического отчета, предоставляющего консолидированные сведения о компонентах и настройке системы. Эти сведения полезны для поиска и устранения неполадок, а также для диагностики проблем с системой. Этот технический отчет должен быть предоставлен в техническую службу Numa Edge при подаче заявки.

Примеры

В примере выводится первый экран технического отчета.

Пример 80– Отображение консолидированных сведений о системе

```
admin@edge:~$ show tech-support | less
```

```
----------------
Show Tech-Support
----------------

----------------
Serial
----------------
00001.1

----------------
CONFIGURATION
----------------

----------------
Full version
----------------
Numa Edge 1.0.0 FW

----------------
Full apdate info
----------------
Канал                                       Ревизия
================================================================================
==
edge-1.0-amd64/fw                           0/0
geoip/1.0                                   0
 * Ошибка обработки сертификата /etc/apdc/cert.pem
Подписка                                    Дата окончания
================================================================================
==

----------------
Internal build
----------------
Mon Dec 14 05:25:22 MSK 2020
commit 3f92dc9198365ff65d9c6ad2a16cc229ca9d0ba8

----------------
Configuration File
----------------
```

7.3.82 show version

Отображение сведений о сертификационной версии программного обеспечения.

Синтаксис

```
show version
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Примеры

В примере ниже показан образец вывода команды show version без параметров.

Пример 81– Отображение сведений о версии

```
admin@edge:~$ show version
```

```
Numa Edge 1.0 FW
admin@edge:~$
```

7.3.83 shutdown

Выключение системы.

Синтаксис

```
shutdown [at <время> | cancel | now]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

at *время*

Время, на которое запланирована перезагрузка системы. Дата и, при необходимости, время устанавливаются непосредственно в одном из следующих форматов:

- +ММ
- ЧЧ:ММ

cancel

Отмена перезагрузки, ранее поставленной в расписание.

now

Перезагрузка системы без подтверждения

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для выключения системы.

Перед перезагрузкой системы всем вошедшим в систему пользователям рассылается вещательное сообщение, предупреждающее их о перезагрузке. В том случае если указывается момент времени меньше текущего без указания даты, перезагрузка системы планируется в указанный момент времени следующего дня. В том случае если указывается дата без указания времени, перезагрузка планируется на 00 часов 00 минут указанного дня.

7.3.84 system back-up to <архив>

Данная команда осуществляет сохранение состояния устройства: конфигурацию, а так же другие файлы, необходимые для корректного восстановления конфигурации, в указанный архив.

Синтаксис

system back-up to <архив>

Режим интерфейса

Эксплуатационный режим.

Параметры

архив

Имя файла архива, включая полный путь к его месту сохранения.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для выключения системы.

Данная команда используется для сохранения состояния устройства в указанный архив. Итоговый файл позже может быть загружен в работающую систему с целью замены текущего состояния устройства с помощью команды `system restore from <архив>`.

Каталогом для сохранения по умолчанию является домашний каталог пользователя, из-под которого выполняется данная команда. Так же возможно сохранение на жесткий диск по пути, отличающемуся от стандартного каталога `/home/<user>`, внешний накопитель (например, USB-флеш-накопителя), удаленное устройство по протоколам FTP, TFTP или SCP. Перед тем, как состояние устройства можно будет сохранить на флэш-накопитель, последний следует проинициализировать командой flash init в эксплуатационном режиме.

В таблице приведен синтаксис способов указания пути для восстановления состояния устройства из архива.

Таблица 22 – Примеры указания временного значения

Место сохранения	Способ указания
Локально (абсолютный путь)	Используется стандартный способ указания пути к файлу в UNIX: /путь/имя_архива где путь - путь сохранения файла конфигурации, имя_архива – имя файла с состоянием устройства.
Локально (относительный путь)	Указывается имя файла относительно стандартного каталога /home/<user>: имя_архива где имя_архива – имя архива с состоянием устройства.
Удаленно (протокол SCP)	Используется следующий синтаксис: scp://имя_пользователя@хост/имя_архива где хост - IP-адрес или имя удаленного хоста для сохранения архива с состоянием устройства, имя_пользователя - имя пользователя удаленного хоста, имя_архива - имя архива, включая путь на удаленном хосте.
Удаленно (протокол FTP)	Используется следующий синтаксис: ftp://имя_пользователя@хост/имя_архива где хост - IP-адрес или имя удаленного хоста для сохранения архива с состоянием устройства, имя_пользователя - имя пользователя удаленного хоста, имя_архива - имя архива, включая путь относительно корневого каталога FTP.
Удаленно (протокол TFTP)	Используется следующий синтаксис: tftp://хост/имя_архива где хост - IP-адрес или имя удаленного хоста для сохранения архива с состоянием устройства, имя_архива - имя архива, включая путь относительно корневого каталога TFTP.

7.3.85 system clean

Данная команда осуществляет сброс состояния устройства до начального.

Синтаксис

```
system clean
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для сброса состояния устройства до начального. Удаляются ранее сгенерированные сертификаты, файлы лицензий сторонних вендоров, ключи для VPN и собственные правила IDPS в случае их наличия. При выполнении данной команды системный журнал не удаляется.

7.3.86 system detect

Вывод информации об аппаратной платформе и модели устройства.

Синтаксис

```
system detect
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения наименования аппаратной платформы, а также модели устройства Numa Edge.

Примеры

В примере показан вывод команды system detect.

Пример 82– Вывод в консоль при выполнении команды system detect.

```
admin@edge:~$ system detect
Platform NCA-4210B-1, model 200
```

7.3.87 system restore from <архив>

Данная команда осуществляет восстановление состояния устройства: конфигурацию, а так же другие файлы, необходимые для корректного восстановления конфигурации, в указанный архив.

Синтаксис

```
system restore to <архив>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

архив

Имя файла архива, включая полный путь к его месту сохранения.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для восстановления состояния устройства из указанного архива. Архив для восстановления состояния устройства может быть выгружен из работающей системы с помощью команды system back-up to <архив>.

Каталогом для восстановления по умолчанию является домашний каталог пользователя, из-под которого выполняется данная команда. Так же возможно восстановление из архива, расположенного на: жестком диске по пути, отличающемуся от стандартного каталога /home/<user>, внешнем накопителе (например, USB-флеш-

накопитель), удаленном устройстве с помощью протоколов FTP, TFTP или SCP. Перед тем, как состояние устройства можно будет восстановить из на флэш-накопитель, последний следует проинициализировать командой flash init в эксплуатационном режиме.

В таблице приведен синтаксис способов указания пути для восстановления состояния устройства из архива.

Таблица 23 – Способы указания пути для сохранения файла конфигурации

Место сохранения	Способ указания
Локально (абсолютный путь)	Используется стандартный способ указания пути к файлу в UNIX: /путь/имя_архива где путь - путь сохранения файла конфигурации, имя_архива – имя файла с состоянием устройства.
Локально (относительный путь)	Указывается имя файла относительно стандартного каталога /home/<user>: имя_архива где имя_архива – имя архива с состоянием устройства.
Удаленно (протокол SCP)	Используется следующий синтаксис: scp://имя_пользователя@хост/имя_архива где хост - IP-адрес или имя удаленного хоста для восстановления состояния устройства из архива, имя_пользователя - имя пользователя удаленного хоста, имя_архива - имя архива, включая путь на удаленном хосте.
Удаленно (протокол FTP)	Используется следующий синтаксис: ftp://имя_пользователя@хост/имя_архива где хост - IP-адрес или имя удаленного хоста для восстановления состояния устройства из архива, имя_пользователя - имя пользователя удаленного хоста, имя_архива - имя архива, включая путь относительно корневого каталога FTP
Удаленно (протокол TFTP)	Используется следующий синтаксис: tftp://хост/имя_архива где хост - IP-адрес или имя удаленного хоста для восстановления состояния устройства из архива, имя_архива - имя архива, включая путь относительно корневого каталога TFTP.

7.3.88 system integrity export

Осуществляет выгрузку на съемный флеш-носитель архива с файлами для расчета контрольных сумм.

Синтаксис

```
system integrity export
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда позволяет осуществить выгрузку на съемный флеш-носитель архива с файлами для рассчета контрольных сумм в соответствии с инструкцией 643.АМБН.00004-01 88 01 "Инструкция по проверке контрольных сумм".

Примеры

В примере показан частичный вывод команды system integrity export для системы edge.

Пример 83– Вывод в консоль при выполнении команды system integrity export.

```
admin@edge:~$ system integrity export
Mounting formatted drive...   done
bin/hostname.busybox
bin/login.util-linux-ng
boot/bzImage-4.19.11
...
usr/sbin/brctl.busybox
usr/sbin/xtables-multi
Attempting to unmount /dev/usbstick...done
admin@edge:~$
```

7.3.89 terminal

Контроль за поведением системного терминала.

Синтаксис

```
terminal [key query-help <состояние> | length <количество_строк> | pager [<команда_просмотра_страниц>] | width <ширина>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

состояние

Установка возможности использования вопросительного знака для получения справки. Допустимые значения:

enable: Разрешить использовать вопросительный знак для получения справки;

disable: Запретить использовать вопросительный знак для получения справки.

По умолчанию разрешено использование вопросительного знака для получения справки.

количество_строк

Установка длины экрана терминала в строках.

команда_просмотр_страниц

Программа, используемая для постраничного просмотра на терминале. Если программа не указана, используется программа по умолчанию (cat).

ширина

Установка ширины экрана терминала на данное число колонок.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта программа используется для установки поведения терминала.

7.3.90 test

Выполнить регламентное тестирование.

Синтаксис

test

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для запуска процедуры регламентного тестирования Numa Edge.

8 Управление пользователями

В этом разделе описана настройка пользователей и аутентификация пользователей. В этом разделе рассматриваются следующие вопросы:

- Настройка управления пользователями
- Команды управления пользователями

8.1 Настройка управления пользователями

В этом разделе рассматриваются следующие вопросы:

- Обзор управления пользователями
- Создание учетных записей пользователей для входа в систему
- Настройка для доступа по SSH с помощью общих открытых ключей

8.1.1 Обзор управления пользователями

Системой Numa Edge поддерживается следующее:

- Аутентификация при входе в систему
- Доступ по SSH с помощью общих открытых ключей

Аутентификация при входе в систему

По умолчанию система создает одну учетную запись пользователя с именем **admin** и паролем **admin**. По соображениям безопасности пароль в дальнейшем настоятельно рекомендуется сменить. Система проверяет подлинность пользователей по паролю, настроенному с помощью команды **system login user** <**пользователь**> **authentication**.

Для управления учетными записями пользователей следует использовать команды системы конфигурирования во избежание возможных проблем.

Узел конфигурации **login** является обязательным узлом. Он создается автоматически и заполняется сведениями по умолчанию при первом запуске системы. Если этот узел впоследствии удаляется, система воссоздает его при перезапуске с заполнением по умолчанию.

Пароли пользователей для входа вводятся открытым текстом. После фиксации настройки система шифрует их и сохраняет внутри себя зашифрованные версии. При отображении настройки пользователя отображается только зашифрованная версия пароля.

ПРИМЕЧАНИЕ В Numa Edge используются следующие ограничения для попыток перебора пароля:
- ограничение до 5 попыток неправильного ввода пароля для указанного пользователя
- после каждой из первых пяти ошибок происходит задержка на 3 секунды;
- после 5 неуспешных попыток авторизации учетная запись блокируется на 5 минут
- каждая последующая попытка авторизации для заблокированного пользователя, вне зависимости от правильности ввода пароля, обнуляет таймер блокировки

Доступ по SSH с помощью общих открытых ключей

Удаленный доступ к операционной системе Numa Edge, как правило, устанавливается через SSH. SSH позволяет обеспечить защищенный сеанс, однако при использовании SSH существует одна потенциальная проблема, которая заключается в том, что если для проверки подлинности используется пароль, то его возможно подобрать. В качестве альтернативы аутентификации по паролю, не подверженной этому риску, для проверки подлинности по SSH пользователи используют общие открытые ключи.

При использовании этого метода удалённой системой создается пара из закрытого и открытого ключей (обычно с помощью команды Linux **ssh-keygen**). Файл открытого ключа (как правило, с расширением .**pub**) загружается в настройку входа в систему пользователя, который сможет получить доступ к системе, используя его с помощью команды **loadkey**. Кроме того, в настройке системы Numa Edge должна быть отключена аутентификация по SSH с использованием пароля. Таким образом, пользователи SSH могут быть

аутентифицированы с использованием паролей или общих открытых ключей, но не того и другого одновременно.

8.1.2 Создание учетных записей пользователей для входа в систему

В этом разделе представлен пример настройки учетной записи пользователя, проходящего проверку подлинности с использованием локальной пользовательской базы данных. Образец настройки приведен на рисунке.

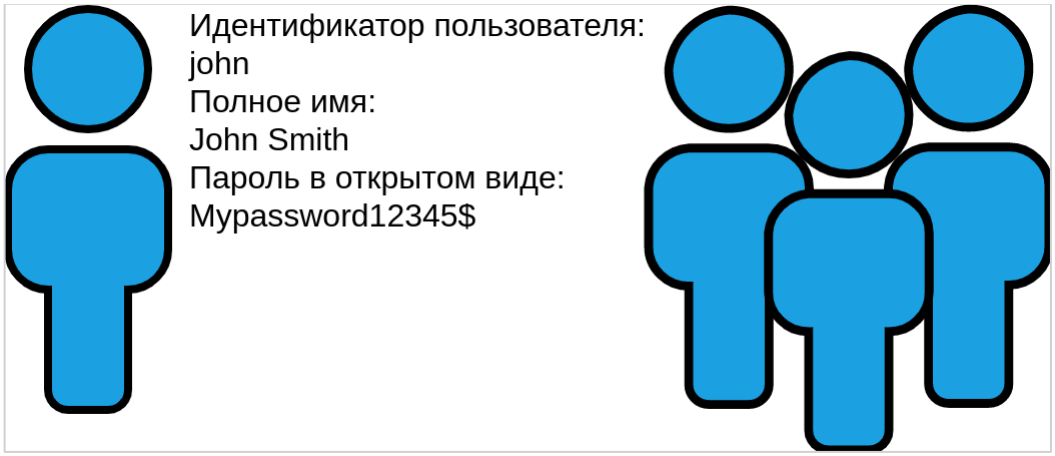


Рисунок 6 – Учетная запись пользователя для входа в систему

В этом примере выполняется создание пользовательской учетной записи для **John Smith**. John имеет пользовательский идентификатор **john** и будет использовать пароль **Mypassword12345$**. Следует обратить внимание, что после фиксации настройки при ее выводе будет отображаться только зашифрованная версия пароля.

ПРИМЕЧАНИЕ Задаваемый пароль должен соответствовать требованиям безопасности: быть длиной не менее 10 символов, содержать по крайней мере одну букву в верхнем регистре, содержать по крайней мере одну цифру.

Для создания учетной записи пользователя, предназначенной для входа в систему, выполните следующие действие в режиме настройки:

Пример 84– Создание учетной записи пользователя для входа в систему

Действие	**Команда**
Создание узла конфигурации user, указание идентификатора пользователя и его полного имени.	`[edit]` `admin@Edge1# set system login user john full-name "John Smith"`
Указание пароля пользователя открытым текстом.	`[edit]` `admin@Edge1# set system login user john authentication plaintext-password Mypassword12345$`
Фиксация изменения. После фиксации пароля он может быть отображен только в зашифрованной форме как значение атрибута encrypted-password.	`[edit]` `admin@Edge1# commit`

Отображение содержимого узла конфигурации system login.	`admin@Edge1# show system login`
	`user admin {`
	`authentication {`
	`encrypted-password`
	`$1$EyOd.0dr$j74/m/yLATcXqeiI5zKPR0`
	`plaintext-password ""`
	`}`
	`level admin`
	`}`
	`user john {`
	`authentication {`

Действие	Команда
	encrypted-password 1lU4LWpp9$qJFg8uNfXrZbNzQrUtDXc. plaintext-password "" } full-name "John Smith" } [edit] admin@Edge1#

8.1.3 Настройка для доступа по SSH с помощью общих открытых ключей

В данном разделе приведен пример настройки доступа по SSH с помощью общих открытых ключей, как показано ниже.

Рисунок 7 – Доступ по SSH с использованием общих открытых ключей

В этом примере выполняется настройка системы Numa Edge для доступа по SSH с использованием общих открытых ключей для аутентификации; аутентификация по паролю при этом отключается (хотя отключение аутентификации по паролю не является предварительным условием для использования общих открытых ключей для аутентификации). В данном случае пользователь **John Smith** (username = **john**) уже существует в системе. Кроме того, открытый ключ (**xxx.pub**) уже создан (при помощи команды Linux **ssh-keygen**) и находится в каталоге, владельцем которого является пользователь **j2** на узле **xyz.abc.com**.

Для настройки доступа по SSH с использованием общих открытых ключей нужно выполнить следующие действия в режиме настройки:

Пример 85– Настройка доступа по SSH с использованием общих открытых ключей

Действие	Команда
Загрузка общего открытого ключа (**xxx.pub**) с системы, где он находится, и связывание его с пользователем **john**. В данном случае ключ расположен на машине **xyz.abc.com** в каталоге, владельцем которого является пользователь **j2**.	[edit] admin@Edge1# loadkey john scp://j2@xyz.abc.com/home/j2/.ssh/xxx.pub j2@xyz.abc.com's password: xxx.pub Done
Отключение аутентификации по паролям для SSH в системе. Следует обратить внимание, что это действие не является строго необходимым, но желательно, если пользователи должны использовать только проверку подлинности по общему открытому ключу.	[edit] admin@Edge1# set service ssh disable- password-authentication true
Фиксация изменения.	[edit] admin@Edge1# commit
Отображение изменения.	[edit] admin@Edge1# show service ssh disable-password-authentication true
Сохранение настройки для сохранения состояния изменений после перезагрузки.	[edit] admin@Edge1# save Saving configuration to '/etc/config/config.boot'... Done
Отображение изменения.	admin@Edge1# show system login

Действие	Команда

	user admin {
	authentication {
	encrypted-password
	1EyOd.0dr$j74/m/yLATcXqeiI5zKPR0
	plaintext-password ""
	}
	level admin
	}
	user john {
	authentication {
	encrypted-password
	1uHMDtq.u$.o48yjWAcxOgMBZYoOYZk1
	plaintext-password ""
	public-keys j2@xyz.abc.com {
	key
	AAAAB3NzaC1yc2EAAAADAQABAAABAQDDpoShD8lCrlO9h
	BP+gumcPV+BMquOrBwkDlvJ/UMcOKJ0NjLZK59FZ+SUsM
	g+xTPJRCqJYUDEPa07qS4gz1xDKIGsU5TP2CIXjcdfFp
	type ssh-rsa
	}
	}
	full-name "John Smith"
	}

8.2 Команды управления пользователями

Команды настройки	
loadkey	Загрузка общего открытого ключа для пользователя SSH.
system login	Создание узла конфигурации для управления пользователями и проверки их подлинности.
system login banner post-login <сообщение>	Указание заставки для отображения после входа в систему.
system login banner pre-login <сообщение>	Указание заставки для отображения перед входом в систему.
system login expiry pwd-change <количество_дней>	Данная команда позволяет указать максимальный период действия пароля пользователя для всех учетных записей в системе.
system login expiry pwd-change-warn <количество_дней>	Данная команда позволяет указать, за сколько дней до истечения действия пароля необходимо выдавать предупреждение пользователям.
system login ldap enabled <режим>	Включение авторизации пользователей Numa Edge на основе LDAP.
system login ldap mapping <схема_сопоставления_атрибутов>	Указание схему сопоставления атрибутов, в соответствии с которой проводится авторизации LDAP
system login user <пользователь>	Создание учетной записи пользователя.
system login user <пользователь> authentication	Установка пароля проверки подлинности для пользователя.
system login user <пользователь> authentication public-keys	Указание параметров проверки подлинности пользователя с помощью общего открытого ключа для SSH.
system login user <пользователь> expiry account-lock-on <дата>	Данная команда позволяет указать дату окончания периода действия учетной записи пользователя.
system login user <пользователь> expiry pwd-change <количество_дней>	Данная команда позволяет указать максимальный период действия пароля пользователя.
system login user <пользователь> expiry pwd-change-warn <количество_дней>	Данная команда позволяет указать, за сколько дней до истечения действия пароля необходимо выдавать предупреждение пользователю.
system login user <пользователь> full-name <имя>	Запись полного имени пользователя.
system login user <пользователь> group <группа>	Внесение пользователя в группу.

system login user <пользователь> level <уровень>	Указание уровня полномочий и прав доступа к системе для пользователя.
Эксплуатационные команды	
show system login users	Отображение учетных сведений о пользователях.
show user <имя_пользователя>	Вывод сведений о последнем входе пользователя в систему, а также о настройках периода действия пароля и учетной записи пользователя.
show users	Вывод списка пользователей, в настоящее время вошедших в систему.

8.2.1 loadkey

Загрузка общего открытого ключа для пользователя SSH.

Синтаксис

```
loadkey <пользователь> <имя_файла>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

Отсутствует.

Параметры

пользователь

Имя пользователя, которое следует связать с общим открытым ключом. Пользователь должен быть уже определен в системе Numa Edge.

имя_файла

Имя файла общего открытого ключа, в том числе полный путь к его местоположению. Файлы общего открытого ключа обычно создаются на удаленной системе с помощью команды Linux **ssh-keygen** и имеют имена с расширением .**pub**. В них содержатся тип аутентификации (например, **ssh-gost2012**), строка значения ключа и идентификатор пользователя удаленной системы (например, **john@example.com**).

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для загрузки общего открытого ключа для SSH из файла в настройку **public-keys** для пользователя (см. команду system login user <пользователь> authentication public-keys). Это позволяет не вводить общий открытый ключ вручную

ПРИМЕЧАНИЕ Данную команду можно выполнять только при отсутствии незафиксированных изменений.

Общий открытый ключ, созданный в удаленной системе, можно загрузить с жесткого диска (в том числе с флэш-накопителя или накопителя для порта USB) или с сервера TFTP, FTP, SCP или HTTP.

Если загружается открытый ключ, содержащий идентификатор пользователя удаленной системы, совпадающий с существующим именем пользователя в **public-keys**, существующий ключ будет перезаписан.

В приведенной ниже таблице показан синтаксис указания файла для различных местоположений файла.

Таблица 24 – Способы указания местоположения для файла общего открытого ключа

Местоположение	**Способ указания**
Абсолютный путь	Используется стандартный способ указания файла в UNIX.
Относительный путь	Указывается имя файла с путем относительно каталога конфигурации по умолчанию.
Сервер SCP	Используется следующий синтаксис для параметра *имя_файла*: **scp:**//*пользователь@узел/файл_ключа*, где *пользователь* это имя пользователя на узле, *узел* это имя узла или IP-адрес сервера SCP, а *файл_ключа* это файл, содержащий

Местоположение	Способ указания
	открытый ключ, включая путь. Если *пользователь* не указан, будет выдан запрос на его ввод. Если аутентификация производится по паролю, далее будет запрошен пароль.
Сервер HTTP	Используется следующий синтаксис для параметра *имя_файла*: **http:**//*узел*/*файл_ключа*, где *узел* это имя узла или IP-адрес сервера HTTP, а *файл_ключа* это файл ключа, включая путь.
Сервер TFTP	Используется следующий синтаксис для параметра *имя_файла*: **tftp:**//*узел*/*файл_ключа* где *узел* это имя узла или IP-адрес сервера TFTP, а *файл_ключа* это файл ключа, включая путь относительно корневого каталога TFTP.

Примеры

В примере открытый ключ для авторизации пользователя **john** в системе Edge1 загружается из каталога, владельцем которого является пользователь **j2** на узле **xyz.abc.com**.

Пример 86– Загрузка открытого ключа с удаленного узла

```
admin@Edge1# loadkey john scp://j2@xyz.abc.com/home/j2/.ssh/xxx.pub
j2@xyz.abc.com's password:
xxx.pub
Done
admin@Edge1# show system login user john
   authentication {
       encrypted-password $1$lU4LWpp9$qJFg8uNfXrZbNzQrUtDXc.
       plaintext-password ""
       public-keys j2@xyz.abc.com {
           key
AAAAB3NzaC1yc2EAAAADAQABAAABAQDDpoShD8lCrlO9hBP+gumcPV+BMquOrBwkDlvJ/UMcOKJ0Nj
LZK59FZ+SUsMg+xTPJRCqJYUDEPa07qS4gz1xDKIGsU5TP2CIXjcdfFp
           type ssh-rsa
       }
   }
   full-name "John Smith"
[edit]
admin@Edge1#
```

8.2.2 system login

Создание узла конфигурации для управления пользователями и проверки их подлинности.

Синтаксис

```
set system loginshow system login
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   login {
   }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда с ее подкомандами используется для управления учетными записями пользователей, а также аутентификацией пользователей. Узел конфигурации **login** является обязательным узлом. Он создается автоматически и заполняется сведениями по умолчанию при первом запуске системы. Если этот узел впоследствии удаляется, система воссоздает его с заполнением по умолчанию. Форма **set** этой команды используется для создания узла конфигурации **login**.

Форма **show** этой команды используется для просмотра сведений о пользователях, а также об аутентификации пользователей.

ПРИМЕЧАНИЕ Обратите внимание, что для данной команды не предусмотрена форма delete. Попытка выполнить удаление узла system login завершится ошибкой, так как в системе должна присутствовать по крайней мере одна учетная запись для входа.

8.2.3 system login banner post-login <сообщение>

Указание сообщения для отображения после входа в систему.

Синтаксис

```
set system login banner post-login <сообщение>
delete system login banner post-login
show system login banner post-login
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    login {
        banner {
            post-login сообщение
        }
    }
}
```

Параметры

сообщение

Сообщение, выводимое пользователю после успешного входа в систему. Строка должна быть заключена в двойные кавычки. Кроме того, можно вводить специальные символы типа перехода на новую строку (\n) и табуляции (\t).

Значение по умолчанию

Система отображает сведения о времени последнего входа в систему.

Указания по использованию

Эта команда используется для указания текста, который появится на экране при удачном входе пользователя в систему.

Форма **set** этой команды используется для указания сообщения для отображения после входа в систему.

Форма **delete** этой команды используется для возврата к сообщению по умолчанию после входа в систему.

Форма **show** этой команды используется для просмотра настройки сообщения для отображения после входа в систему.

8.2.4 system login banner pre-login <сообщение>

Указание сообщения для отображения перед входом в систему.

Синтаксис

```
set system login banner pre-login <сообщение>
delete system login banner pre-login
show system login banner pre-login
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   login {
      banner {
         pre-login сообщение
      }
   }
}
```

Параметры

сообщение

Сообщение, выводимое пользователю перед входом в систему. Строка должна быть заключена в двойные кавычки. Кроме того, можно вводить специальные символы типа перехода на новую строку (\n) и табуляции (\t).

Значение по умолчанию

Система отображает приветственное сообщение.

Указания по использованию

Эта команда используется для указания текста, который появится на экране при вводе пользователем своего имени входа и пароля.

Форма **set** этой команды используется для указания сообщение для отображения перед входом в систему.

Форма **delete** этой команды используется для возврата к сообщению по умолчанию после входа в систему.

Форма **show** этой команды используется для просмотра настройки сообщения для отображения перед входом в систему.

8.2.5 system login expiry pwd-change <количество_дней>

Данная команда позволяет указать максимальный период действия пароля пользователя для всех учетных записей в системе.

Синтаксис

```
set system login expiry pwd-change <количество_дней>
delete system login expiry pwd-change
show system login expiry pwd-change
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   login {
     expiry {
         pwd-change количество_дней
     }
```

```
    }
}
```

Параметры

количество_дней

Период действия пароля пользователя в днях. По истечении заданного количества дней пароль пользователя становится недействительным.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда позволяет задавать период действия пароля пользователя для всех учетных записей пользователя в системе. По умолчанию пароль пользователя имеет неограниченный период действия.

ПРИМЕЧАНИЕ Пароль действует на один день больше чем указано, таким образом, при указании периода действия пароля равным 1 дню, пароль будет действителен в день смены пароля, а также до 23.59 следующего дня.

При использовании ограниченного периода действия пароля удобно настроить также напоминание о необходимости смены пароля, это можно сделать при помощи команды **system login expiry pwd-change-warn количество_дней**.

ПРИМЕЧАНИЕ Смена пароля пользователя возможна только в конфигурации учетной записи пользователя, таким образом, если период действия пароля пользователя истек и пароль заблокирован, изменить его может только другой пользователь, обладающий правами администратора.

Форма **set** этой команды используется для указания периода действия пароля пользователя для всех учетных записей в системе.

Форма **delete** этой команды предназначена для настройки периода действия пароля пользователя для всех учетных записей.

Форма **show** этой команды предназначена для просмотра настройки периода действия пароля пользователя для всех учетных записей в системе.

8.2.6 system login expiry pwd-change-warn <количество_дней>

Данная команда позволяет указать, за сколько дней до истечения действия пароля необходимо выдавать предупреждение пользователям.

Синтаксис

```
set system login expiry pwd-change-warn <количество_дней>
delete system login expiry pwd-change-warn
show system login expiry pwd-change-warn
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    login {
        expiry {
            pwd-change-warn количество_дней
        }
    }
}
```

Параметры

количество_дней

Количество дней до истечения периода действия пароля, за которое пользователю начинает выдаваться предупреждение.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда позволяет настроить вывод предупреждений всем пользователям системы с указанием количества дней, оставшихся до истечения периода действия пароля. Предупреждение выдается пользователю при использовании интерфейса командной строки (при подключении через SSH или последовательный порт) при входе в систему. По умолчанию предупреждения не выводятся.

Период действия пароля для всех учетных записей в системе указывается при помощи команды **system login expiry pwd-change количество_дней**.

ПРИМЕЧАНИЕ В день смены пароля предупреждения не выводятся. Также предупреждения не выводятся в последний день периода действия пароля.

Форма **set** этой команды позволяет указать, за сколько дней до истечения действия пароля необходимо выдавать предупреждение пользователю.

Форма **delete** этой команды предназначена для удаления сообщения с предупреждением о смене пароля.

Форма **show** этой команды предназначена для просмотра настройки.

8.2.7 system login ldap enabled <режим>

Включение авторизации пользователей Numa Edge на основе LDAP.

Синтаксис

```
set system login ldap enabled <режим>
delete system login ldap enabled
show system login ldap enabled
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    login {
        ldap {
            enabled режим
        }
    }
}
```

Параметры

режим

Допустимые значения:

true: авторизация пользователей Numa Edge на основе LDAP включена.

false: авторизация пользователей Numa Edge на основе LDAP выключена.

Значение по умолчанию

Авторизация пользователей Numa Edge на основе LDAP выключена.

Указания по использованию

Эта команда позволяет включить авторизацию пользователей Numa Edge на основе LDAP.

ПРИМЕЧАНИЕ Для корректной работы данного параметра в системе Numa Edge должно быть настроено подключение к серверу LDAP с использованием ветви конфигурации **system ldap-server**

ОБРАТИТЕ ВНИМАНИЕ Пользователи, чей номер уникального идентификатора меньше 10 000, будут проигнорированы при попытке авторизации.

На сервере LDAP требуется создание класса **nisNetgroup** с названием edge-admin и/или edge-op. В объекте *nisNetgroup* необходимо создание атрибута **nisNetgroupTriple**, в формате:

(,пользователь,)

Если имя класса *nisNetgroup* - edge-admin, пользователь, указанный в атрибуте *nisNetgroupTriple* будет авторизован как локальный администратор.

Если имя класса *nisNetgroup* - edge-op, пользователь, указанный в атрибуте *nisNetgroupTriple* будет авторизован как локальный оператор.

Другим обязательным условием авторизации является указание домашнего каталога в атрибуте **unixHomeDirectory** для каждого пользователя.

Форма **set** этой команды используется для включения авторизации пользователей Numa Edge на основе LDAP.

Форма **delete** этой команды используется для удаления настройки и восстановления значения, принятого по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

8.2.8 system login ldap mapping <схема_сопоставления_атрибутов>

Указание схемы сопоставления атрибутов LDAP, используемой при авторизации пользователей в системе Numa Edge.

Синтаксис

```
set system login ldap mapping <схема_сопоставления_атрибутов>
delete system login ldap mapping
show system login ldap mapping
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    login {
        ldap {
            mapping схема_сопоставления_атрибутов
        }
    }
}
```

Параметры

схема_сопоставления_атрибутов

Схема, определяющая перечень наименований атрибутов, используемая на удаленном сервере LDAP. Допустимые значения представлены в таблице ниже:

Таблица 25 – Схемы сопоставления атрибутов LDAP

Значение	Описание
rfc2307	Схема, соответствующая RFC 2307
sfu20	Схема, соответствующая Microsoft Services for UNIX 2.0
sfu35	Схема, соответствующая Microsoft Services for UNIX 3.5
Ad	Схема, соответствующая Microsoft Active Directory
Aix	Схема, соответствующая AIX SecureWay

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда позволяет указать какая схема именования атрибутов используется на удаленном сервере LDAP, к которому выполняется подключение.

ПРИМЕЧАНИЕ для корректной работы данного параметра в системе Numa Edge должно быть настроено подключение к серверу LDAP с использованием ветви конфигурации system ldap-server

Форма **set** этой команды используется указания имени схемы соответствия атрибутов, которая используется при авторизации пользователей Numa Edge.

Форма **delete** этой команды используется для удаления настройки и восстановления значения, принятого по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

8.2.9 system login user <пользователь>

Создание учетной записи пользователя.

Синтаксис

```
set system login user <пользователь>
delete system login user <пользователь>
show system login user <пользователь>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   login {
      user пользователь {
      }
  }
}
```

Параметры

пользователь

Множественный узел. Уникальный идентификатор пользователя длиной до 32 символов включительно, допускаются алфавитно-цифровые символы и дефисы. Можно определить несколько учетных записей пользователей, создав несколько узлов конфигурации **user**.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения пользователя, подлинность которого будет проверяться с помощью встроенного механизма системы - аутентификации при входе в систему.

Форма **set** этой команды используется для создания узла конфигурации **user**.

Форма **delete** этой команды используется для удаления узла конфигурации **user**. Следует обратить внимание на то, что нельзя удалить текущую учетную запись, последнюю учетную запись в системе, последнюю учетную запись администратора в системе.

Форма **show** этой команды используется для просмотра настройки **user**.

8.2.10 system login user <пользователь> authentication

Установка пароля проверки подлинности для пользователя.

Синтаксис

```
set system login user user authentication [encrypted-password <заш_пароль> | plaintext-password <откр_пароль>]

delete system login user user authentication [encrypted-password | plaintext-password]

show system login user user authentication [encrypted-password | plaintext-password]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    login {
        user пользователь {
            authentication {
                encrypted-password заш_пароль
                plaintext-password откр_пароль
            }
        }
    }
}
```

Параметры

пользователь

Идентификатор пользователя.

заш_пароль

Зашифрованный пароль. Это значение создано системой, и изменять его не следует.

откр_пароль

Пароль пользователя открытым текстом. Допустимо большинство специальных символов за исключением одиночной кавычки, двойной кавычки и обратной косой черты ("\"). В том случае если пароль содержит символ "$", он должен быть заключен в одинарные кавычки, например, '564$jhgJ48'.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки пароля, используемого пользователем для аутентификации в консоли управления (а также веб-интерфейсе) Numa Edge.

Требования к устанавливаемым паролям:

- пароль должен быть не менее 10 символов.
- пароль должен содержать, по крайней мере, одну букву в нижнем регистре.
- пароль должен содержать, по крайней мере, одну букву в верхнем регистре.
- пароль должен содержать, по крайней мере, одну цифру.
- Пароль должен соответствовать требованиям к сложности:
    - не быть словарным паролем и не содержать словарные фразы (в том числе написанные наоборот);
    - содержать не менее 5 различных символов;
    - не содержать большого числа пар символов идущих подряд в алфавите (например, ab, dc, xy, zy).

ПРИМЕЧАНИЕ Максимальное число таких пар в пароле может быть 3, плюс по одной паре на примерно каждые 12 символов пароля, таким образом:

- для пароля длинной 11 символов - не более 3 пар;
- для пароля длинной 12 символов - не более 4 пар;
- для пароля длинной 24 символа - не более 5 пар.

ПРИМЕЧАНИЕ Задаваемые пароли не хранятся в открытом виде в конфигурации изделия – при фиксировании конфигурации введенное значение объединяется со случайно сгенерированной строкой данных и хешируется, а полученный результат помещается в узел конфигурации **encrypted-password**. При этом команды содержащие ввод пароля в открытом виде не сохраняются в истории команд.

Для отключения учетной записи пользователя без ее удаления можно просто установить значение параметра **encrypted-password** в «*».

Форма **set** этой команды используется для установки пароля пользователя.

Форма **delete** этой команды используется для удаления пароля пользователя.

ПРИМЕЧАНИЕ Фиксация полного удаления узла authentication завершится ошибкой, так как вход в систему без подтверждения запрещен.

Форма **show** этой команды используется для просмотра настройки пароля пользователя.

8.2.11 system login user <пользователь> authentication public-keys

Указание параметров аутентификации пользователя для SSH на основе асимметричной ключевой пары.

Синтаксис

```
  set system login user пользователь authentication public-keys <ид_ключа> [key
<значение_ключа> | options <параметры_ключа> | type <тип_ключа>]

  delete system login user <пользователь> authentication public-keys <ид_ключа>
[key | options | type]

  show system login user <пользователь> authentication public-keys <ид_ключа>
[key | options | type]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    login {
        user пользователь {
            authentication {
                public-keys ид_ключа {
                    key значение_ключа
                    options параметры_ключа
                    type тип_ключа
                }
            }
        }
    }
}
```

Параметры

пользователь

Идентификатор пользователя.

ид_ключа

Идентификатор ключа. Обычно он имеет вид пользователь@узел и создается при использовании команды **ssh-keygen** для создания пары открытого и закрытого ключей.

значение_ключа

Строка общего открытого ключа.

параметры ключа

Дополнительные параметры для открытого ключа.

тип_ключа

Тип открытого ключа, определяющий метод проверки при аутентификации. Этот параметр должен быть указан обязательно. Допустимые значения указаны в таблице ниже:

Таблица 26 – Поддерживаемые типы открытых ключей

Значение	Описание
ssh-gost2012-256-cpa	Открытый ключ длины 256 бит по алгоритму ГОСТ Р 34.10-2012 с использованием paramset id-GostR3410-2001-CryptoPro-A-ParamSet
ecdsa-sha2-nistp256	Открытый ключ длины ECDSA с NIST P-256 curve.
rsa-sha2-256	Открытый ключ по алгоритму RSA с SHA-512.
rsa-sha2-512	Открытый ключ по алгоритму RSA с SHA-256.
ssh-ed25519	Открытый ключ EdDSA с curve25519.
ssh-rsa	Открытый ключ по алгоритму RSA с SHA-1.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда позволяет указать параметры для использования аутентификации на основе асимметричной ключевой пары при входе в систему по SSH. При фиксации эти значения помещаются в файл

/**home**/<*пользователь*>/.**ssh**/**authorized_keys**. Изменения в этот файл можно вносить только с помощью данной команды.

Рекомендуется не изменять эти параметры непосредственно с помощью формы **set** данной команды, а использовать команду **loadkey**. Эта команда заполнит аргументы **key-id**, **key-value**, **key-options** и **key-type** для указанного пользователя по файлу открытого ключа, созданному командой Linux **ssh-keygen** в удаленной системе

Аутентификация на основе асимметричной ключевой пары для SSH может использоваться наряду с аутентификацией по паролю или самостоятельно. Если присутствуют оба метода одновременно, то запрос на ввод пароля при входе в систему появится только в том случае, если клиент не сможет быть аутентифицирован на основе асимметричной ключевой пары. Чтобы использовать только аутентификацию пользователей на основе асимметричной ключевой пары, необходимо отключить проверку подлинности по паролю для SSH.

Форма **set** этой команды используется для установки параметров ключевой пары.

Форма **delete** этой команды используется для удаления параметров ключевой пары.

Форма **show** этой команды используется для просмотра параметров ключевой пары.

8.2.12 system login user <пользователь> expiry account-lock-on <дата>

Данная команда позволяет указать дату окончания периода действия учетной записи пользователя.

Синтаксис

```
set system login user <пользователь> expiry account-lock-on <дата>
delete system login user <пользователь> expiry account-lock-on
show system login user <пользователь> expiry account-lock-on
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    login {
        user пользователь {
            expiry {
                account-lock-on дата
            }
        }
    }
}
```

Параметры

пользователь

Идентификатор пользователя.

дата

Дата окончания периода действия учетной записи. Значение должно быть указано в следующем формате: ГГГГ.ММ.ДД.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания окончания периода действия учетной записи пользователя. По умолчанию создается учетная запись пользователя с неограниченным периодом действия.

Указанная дата является последним днем, когда учетная запись действительна. Начиная со следующего дня учетная запись блокируется.

Форма **set** этой команды используется для указания даты окончания действия учетной записи пользователя.

Форма **delete** этой команды предназначена для удаления даты окончания периода действия учетной записи пользователя.

Форма **show** этой команды предназначена для просмотра даты окончания периода действия учетной записи пользователя.

8.2.13 system login user <пользователь> expiry pwd-change <количество_дней>

Данная команда позволяет указать максимальный период действия пароля пользователя.

Синтаксис

```
set system login user <пользователь> expiry pwd-change <количество_дней>
delete system login user <пользователь> expiry pwd-change
show system login user <пользователь> expiry pwd-change
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    login {
        user пользователь {
            expiry {
                pwd-change количество_дней
            }
        }
    }
}
```

Параметры

пользователь

Идентификатор пользователя.

количество_дней

Период действия пароля пользователя в днях. По истечении заданного количества дней пароль пользователя становится недействительным.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда позволяет задавать период действия пароля пользователя. По умолчанию пароль пользователя имеет неограниченный период действия.

ПРИМЕЧАНИЕ Срок действия пароля, указываемый данной командой, имеет приоритет над настройкой срока действия пароля для всех пользователей, устанавливаемой командой **system login expiry pwd-change <количество_дней>**.

ПРИМЕЧАНИЕ Пароль действует на один день больше чем указано, таким образом, при указании периода действия пароля равным 1 дню, пароль будет действителен в день смены пароля, а также до 23.59 следующего дня.

При использовании ограниченного периода действия пароля удобно настроить также напоминание о необходимости смены пароля, это можно сделать при помощи команды **system login user <пользователь> expiry pwd-change-warn <количество_дней>**.

ПРИМЕЧАНИЕ Смена пароля пользователя возможна только в конфигурации учетной записи пользователя, таким образом, если период действия пароля пользователя истек и пароль заблокирован, изменить его может только другой пользователь, обладающий правами администратора.

Форма **set** этой команды используется для указания периода действия пароля пользователя.

Форма **delete** этой команды предназначена для настройки периода действия пароля пользователя.

Форма **show** этой команды предназначена для просмотра настройки периода действия пароля пользователя.

8.2.14 system login user <пользователь> expiry pwd-change-warn <количество_дней>

Данная команда позволяет указать, за сколько дней до истечения действия пароля необходимо выдавать предупреждение пользователю.

Синтаксис

```
set system login user <пользователь> expiry pwd-change-warn <количество_дней>
delete system login user <пользователь> expiry pwd-change-warn
show system login user <пользователь> expiry pwd-change-warn
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    login {
        user пользователь {
            expiry {
                pwd-change-warn количество_дней
            }
        }
    }
}
```

Параметры

пользователь

Идентификатор пользователя.

количество_дней

Количество дней до истечения периода действия пароля, за которое пользователю начинает выдаваться предупреждение.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда позволяет настроить вывод предупреждений пользователю с указанием количества дней, оставшихся до истечения периода действия пароля. Предупреждение выдается пользователю при использовании интерфейса командной строки (при подключении через SSH или последовательный порт) при входе в систему. По умолчанию предупреждения не выводятся.

ПРИМЕЧАНИЕ Срок выдачи предупреждения о смене пароля, указываемый данной командой, имеет приоритет над настройкой срока выдачи предупреждения для всех пользователей, устанавливаемой командой **system login expiry pwd-change-warn <количество_дней>**.

Период действия пароля пользователя указывается при помощи команды **system login user <пользователь> expiry pwd-change <количество_дней>**.

ПРИМЕЧАНИЕ В день смены пароля предупреждения не выводятся. Также предупреждения не выводятся в последний день периода действия пароля.

Форма **set** этой команды позволяет указать, за сколько дней до истечения действия пароля необходимо выдавать предупреждение пользователю.

Форма **delete** этой команды предназначена для удаления сообщения с предупреждением о смене пароля.

Форма **show** этой команды предназначена для просмотра конфигурации.

8.2.15 system login user <пользователь> full-name <имя>

Запись полного имени пользователя.

Синтаксис

```
set system login user <пользователь> full-name <имя>
delete system login user <пользователь> full-name
show system login user <пользователь> full-name
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    login {
      user пользователь {
          full-name имя
       }
    }
}
```

Параметры

пользователь

Идентификатор пользователя.

имя

Строка, представляющая имя пользователя; разрешены алфавитно-цифровые символы, пробел и дефисы. Строку, содержащую пробелы необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для записи полного имени пользователя.

Форма **set** этой команды используется для указания имени пользователя.

Форма **delete** этой команды предназначены для удаления имени пользователя.

Форма **show** этой команды предназначена для просмотра имени пользователя.

8.2.16 system login user <пользователь> group <группа>

Внесение пользователя в группу.

Синтаксис

```
set system login user <пользователь> group <группа>
delete system login user <пользователь> group
show system login user <пользователь> group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   login {
      user пользователь {
         group группа
      }
   }
}
```

Параметры

пользователь

Идентификатор пользователя.

группа

Группа, в состав которой нужно включить пользователя. Группы определяются в каталоге /etc/group.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для включения пользователя в группу. Пользователя можно приписать к нескольким группам, выполнив данную команду по разу для каждой группы, к которой следует приписать данного пользователя.

Форма **set** этой команды используется для включения пользователя в состав указанной группы.

Форма **delete** этой команды используется для удаления пользователя из указанной группы.

Форма **show** этой команды используется для просмотра групп, в состав которых входит данный пользователь.

8.2.17 system login user <пользователь> level <уровень>

Указание уровня полномочий и прав доступа к системе для пользователя.

Синтаксис

```
set system login user <пользователь> level <уровень>
delete system login user <пользователь> level
show system login user <пользователь> level
```

Режим интерфейса
Режим настройки.

Ветвь конфигурации
```
system {
    login {
        user пользователь {
            level уровень
        }
    }
}
```

Параметры
пользователь

Идентификатор пользователя.

уровень

Уровень полномочий пользователя. Поддерживаются следующие значения:

admin: Назначение пользователю полномочий администратора. Пользователь может выполнять любую команду в интерфейсе командной строки Numa Edge или в нижележащей операционной системе.

operator: Назначение пользователю ограниченных полномочий. Пользователь может выполнять эксплуатационные команды в интерфейсе командной строки Numa Edge. Пользователь не может входить в режим настройки или выполнять команды настройки.

Значение по умолчанию
По умолчанию пользователям назначаются административные полномочия.

Указания по использованию
Эта команда используется для назначения пользователю доступа к системе на основе роли. В системе поддерживаются две системные роли:

Административный пользователь. У пользователей, которым назначена роль администратора, есть полный доступ к специфическим для Numa Edge командам как конфигурационного, так и эксплуатационного режима.

Пользователь-оператор. Пользователи, которым назначена роль оператора, имеют доступ к набору эксплуатационных команд Numa Edge, но не имеют доступа к командам настройки.

Форма **set** этой команды используется для установки уровня полномочий пользователя.

Форма **delete** этой команды используется для восстановления уровня полномочий пользователя до уровня по умолчанию.

Форма **show** этой команды используется для просмотра настройки полномочий пользователя.

8.2.18 show system login users

Отображение учетных сведений о пользователях.

Синтаксис
```
show system login users [all | locked | other | edge]
```

Режим интерфейса
Эксплуатационный режим.

Параметры
all

Отображение сведений обо всех учетных записях.

locked

Отображение сведений о заблокированных учетных записях.

other

Отображение сведений о системных и сервисных учетных записях, используемых операционной системой.

edge

Отображение сведений об учетных записях Numa Edge.

Значение по умолчанию

Отображение сведений об учетных записях Numa Edge.

Указания по использованию

Эта команда используется для отображения различных подробностей об учетных записях системы. Она позволяет вывести сведения о времени последнего входа пользователей в систему.

Примеры

В примере выводятся сведения об учетных записях пользователей системы edge.

Пример 87– Отображение сведений об учетных записях пользователей

```
admin@edge:~$ show system login users
Username Type Tty From Last login
Username Type Tty From Last login
admin edge pts/1 192.168.100.1 Wed Oct 31 17:38:38 2018
admin@edge:~$
```

8.2.19 show user <имя_пользователя>

Вывод сведений о последнем входе пользователя в систему, а также о настройках периода действия пароля и учетной записи пользователя.

Синтаксис

```
show user <имя_пользователя>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_пользователя

Имя пользователя, для которого требуется отобразить сведения.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для вывода сведений о последнем входе пользователя в систему, а также о настройках периода действия пароля и учетной записи пользователя.

Примеры

В примере выводятся сведения для учетной записи пользователя с именем **admin**.

Пример 88– Отображение сведений для учетной записи пользователя

```
admin@edge:~$ show user admin
Последний вход в систему: Wed 10 13:55 - 13:55 (00:00)
Последнее изменение пароля: Oct 03, 2018
```

```
Срок действия пароля истекает через (дней): никогда
Срок действия учетной записи истекает: никогда
Максимальное кол-во дней между сменой пароля: никогда
Количество дней с предупреждением перед деактивацией пароля: 0
```

8.2.20 show users

Вывод списка пользователей, в настоящее время вошедших в систему.

Синтаксис

```
show users
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для вывода списка пользователей, вошедших в систему в данный момент.

Примеры

В примере выводятся сведения о пользователях, в настоящий момент вошедших в систему edge.

Пример 89– Отображение сведений о пользователях, вошедших в систему в данный момент

```
admin@edge:~$ show users
USER       TTY      IDLE      TIME             HOST
admin      pts/0    00:00     Oct 11 11:38:36 10.150.150.121
admin@edge:~$
```

9 Регистрация событий

В этом разделе описан механизм регистрации событий (записи в журнал) в Numa Edge и доступные пользователю команды просмотра журналов.

ПРИМЕЧАНИЕ Несмотря на то, что пользователю доступны *команды* просмотра различных журналов, доступность для него каждого отдельно взятого *журнала* определяет администратор безопасности комплекса.

9.1 Настройка регистрации событий

9.1.1 Обзор регистрации событий

Важные события в системе записываются в журнал в виде отдельных сообщений (иногда называемые также сообщениями системного журнала), которые могут выводиться на консоль, сохраняться в базу данных, или пересылаться на внешний сервер системного журнала.

В зависимости от уровня серьезности сообщения, выбираемого для регистрации, в число сообщений системного журнала могут входить уведомления о простых и повседневных действиях, а также предупреждения и сообщения о сбоях и ошибках.

В функции регистрации событий системы Numa Edge используется процесс UNIX **syslog-ng**. Настройка регистрации событий, выполненная из интерфейса командной строки системы, сохраняется в файле **/etc/syslog-ng/edge.conf**.

По умолчанию локальная регистрация событий включена, а сообщения сохраняются в базе данных **/var/log/edge/system.db**.

9.1.2 Типы источников сообщений при регистрации событий

Numa Edge поддерживает стандартные типы источников сообщений системного журнала. Они перечислены ниже. Кроме того, можно избирательно включить регистрацию событий для конкретных компонентов маршрутизации. Эти сведения приведены в разделе «Включение и отключение регистрации событий для конкретных функций».

Таблица 27 – Типы источников сообщений для системного журнала

Тип источника сообщений	Описание
All	Все типы источников сообщений, исключая "mark"
Auth	Проверка подлинности и авторизация
Authpriv	Несистемная авторизация
Cron	Служба cron
Daemon	Системные службы
Kern	Ядро
lpr	Буфер построчного принтера
mail	Подсистема электронной почты
news	Подсистема USENET
security	Подсистема безопасности
syslog	Системная регистрация
user	Прикладные процессы
uucp	Подсистема UUCP
local0	Локальный сервис 0
local1	Локальный сервис 1
local2	Локальный сервис 2
local3	Локальный сервис 3
local4	Локальный сервис 4
local5	Локальный сервис 5
local6	Локальный сервис 6

local7	Локальный сервис 7 (протоколы маршрутизации)

9.1.3 Файлы журналов для регистрации событий

При включенной регистрации событий сообщения системного журнала всегда записываются в базу данных **system.db** в каталоге **/var/log/edge** локальной файловой системы. Кроме того, системные журналы можно отправить на консоль или на сервер, на котором работает служебная программа **syslog** (то есть на сервер системного журнала). Также имеется возможность настроить отправку сообщений о событиях системного журнала на электронную почту.

Для вывода сообщений системного журнала на консоль используется команда **system syslog console**.

Для отправки сообщений системного журнала на удаленный компьютер, на котором работает служебная программа **syslog**, используется команда **system syslog host**.

Для отправки сообщений системного журнала по электронной почте используется команда **system syslog mail-to**.

9.1.4 Местоположение и экспорт журнала

Сообщения записываются в файл журнала **system.db** в каталоге **/var/log/edge** файловой системы Numa Edge. Из этого файла можно производить выгрузку сообщений журнала, удалять определённые записи, также он может очищаться автоматически при заполнении файловой системы, содержащей файл журнала более чем на 90%.

ПРИМЕЧАНИЕ По умолчанию, при заполнении файловой системы, содержащей файл журнала более чем на 90%, просматриваются 25% наименее актуальных записей и производится удаление тех из них, что были выгружены.

По умолчанию, система настроена на максимальный уровень требований безопасности, поэтому применяется политика гарантированной сохранности журнала. Это значит, что система не позволит удалить существующие сообщения журнала до тех пор, пока они не будут экспортированы (выгружены) на внешний носитель. Экспорт журнала производится в формате CSV. Рекомендуется выработать и соблюдать регламент выгрузки сообщений журналов, чтобы заполнение файловой системы журналом не привело к отказу в обслуживании. Для уже выгруженных сообщений возможно ручное или автоматическое (по достижении порога заполнения ФС) удаление.

Система также позволяет переключиться в режим, в котором допускается автоматическое и ручное удаление не выгруженных записей. Этот режим не рекомендуется к применению из-за возможной потери регистрируемых событий, за исключением случаев, когда настроено сохранение сообщений журнала на удалённом компьютере. Такой режим позволяет защитить систему от отказа в обслуживании из-за заполнения ФС журналируемыми данными при отсутствии или несоблюдении регламента выгрузки сообщений журнала.

9.1.5 Уровни серьезности сообщений

При системных событиях создаются сообщения, имеющие различные уровни серьезности, которые зависят от степени их важности для системы.

При настройке уровня серьезности для системного журнала система записывает сообщения журнала с уровнем серьезности не меньше настроенной. Чем ниже указанный уровень серьезности, тем больше подробностей записывается в журналы. Например, если уровень серьезности для журнала настроен как **crit**, система записывает сообщения журнала, имеющие серьезность **crit**, **alert** и **emerg**.

Сообщения журналов, созданные системой Numa Edge, связываются с одними из перечисленных ниже уровней серьезности.

Таблица 28 – Уровни серьезности сообщений

Серьезность	Смысл
emerg	Критическая ситуация. Произошел общий сбой системы или другой серьезный сбой, такой что система непригодна для использования.
alert	Уведомление. Необходимо немедленное вмешательство для предотвращения перехода системы в непригодное для использования состояние, например, произошел сбой сети или имел место несанкционированный доступ к базе данных.
crit	Важнейший. Возникло условие максимальной важности, такое как исчерпание ресурсов,

Серьезность	Смысл
	например, в системе отсутствует свободная память, лимиты загрузки ЦП превзойдены или произошёл аппаратный сбой.
err	Ошибка. Возникло условие ошибки, например, произошел сбой системного вызова. Однако система все еще функционирует.
warning	Предупреждение. Произошло событие, которое может вызвать ошибку, например, передаваемые в функцию недопустимые параметры. За этой ситуацией следует наблюдать.
notice	Замечание. Уведомление о важных событиях в системе, не являющихся ошибками, но требующих внимания.
info	Информационное. По мере появления сообщается об обычных событиях, которые могут представлять интерес.
debug	Уровень отладки. Предоставляются сведения уровня отслеживания.
all	Все. Предоставляются сведения обо всех уровнях. Эквивалентно уровню **debug**.

ПРЕДОСТЕРЕЖЕНИЕ Есть риск ухудшения качества обслуживания. Уровни серьезности **debug** и **all** требовательны к ресурсам. Установка уровня регистрации на **debug** или **all** может вызвать ухудшение функционирования системы.

Необходимо иметь в виду что, при включении отладки в протоколах динамической маршрутизации, необходимо изменить уровень серьезности для потока **local7** на значение **debug**. Данное требование связано с тем, что по умолчанию в системном журнале не фиксируются все сообщения, с уровнем серьезности ниже чем **notice**. И, поскольку отладочные сообщения отправляются с наименьшим уровнем серьезности (**debug**), они не будут записаны в системный журнал. Данное утверждение справедливо также для службы webproxy и некоторых других служб, для которых возможно задание уровня серьезности посылаемых сообщений в системный журнал.

9.1.6 Пример настройки регистрации событий

В примере выполняется настройка отправки сообщений журнала связанных с ядром уровня **warning** и более высоких на удалённую машину в локальной сети с адресом 192.168.10.2, в качестве связки протоколов прикладного и транспортного уровней требуется использовать связку IETF/UDP.

Для этого нужно выполнить следующие действия в режиме настройки:

Пример 90– Настройка записи журнала на удалённой машине о событиях, связанных с ядром, имеющих уровень серьезности warning и выше

Действие	Команда
Указание адреса удаленной машины для записи журнала событий	`[edit]` `admin@edge# set system syslog host RemoteLogServ address 192.168.10.2`
Указание типа сообщений и уровня критичности для записи в журнал на удалённой машине	`[edit]` `admin@edge# set system syslog host RemoteLogServ facility kern level warning`
Указание протокола транспортного уровня	`[edit]` `admin@edge# set system syslog host RemoteLogServ transport udp`
Фиксация настройки	`[edit]` `admin@edge# commit`

Отображение всех настроек узла system syslog host	`[edit]`
	`admin@edge# show system syslog host -all`
	`RemoteLogServ {`
	`address 192.168.10.2`
	`facility kern {`
	`level warning`
	`}`
	`format plain`
	`port auto`
	`protocol ietf`
	`transport udp`

Действие	Команда
	} [edit] admin@edge#

9.1.7 Включение и отключение регистрации событий для конкретных функций

В некоторых модулях маршрутизатора Numa Edge регистрацию которых можно включить и выключить внутри узла конфигурации для данного модуля. При включении регистрации событий для модуля системы сообщения журнала отправляются в те же места назначения, которые настроены для системного журнала.

9.1.8 Регистрация вводимых команд

По умолчанию в Numa Edge ведется регистрация вводимых пользователем команд как для интерфейса командной строки, так и для веб-интерфейса. Сообщения регистрации команд, вводимых пользователем в интерфейсе командной строки, заносятся в журнал регистрации от имени программы **shell** (источник **user**, уровень серьезности **info**). Сообщения регистрации действий по настройке, осуществляемых пользователем в веб-интерфейсе, заносятся в журнал регистрации от имени программы **webgui** (источник **user**, уровень серьезности **info**).

ПРИМЕЧАНИЕ. По умолчанию сообщения источника **user** с уровнем серьезности **info** не попадают в журнал регистрации. Настройка типов сообщений, которые отправляются в главный журнал регистрации событий осуществляется при помощи команды system **syslog global facility <источник> level <уровень>**.

9.2 Команды регистрации событий

В этом разделе представлены следующие команды.

Команды настройки	
system syslog	Настройка служебной программы системного журнала в системе.
system syslog console facility <источник> level <уровень>	Указание типов сообщений, отправляемых на консоль.
system syslog global max-age	Настройка времени жизни записей системного журнала в днях.
system syslog global max-history	Настройка максимального количества записей в системном журнале, хранимых после выгрузки.
system syslog global max-size	Настройка максимального занимаемого места на диске файлом системного журнала.
system syslog global signal-age	Настройка порогового значения срока жизни записей в системном журнале.
system syslog global signal-rate	Установка интервала, используемого для регистрации сигнальных сообщений в системный журнал.
system syslog global signal-size	Настройка порогового значения занимаемого места на диске файлом системного журнала.
system syslog global facility <источник> level <уровень>	Указание типов сообщений, которые будут отправляться в главный файл журнала системы.
system syslog host <имя_узла> address <адрес>	Указание адреса удаленного сервера системного журнала.
system syslog host <имя_узла> facility <источник> level <уровень>	Указание типов сообщений, которые будут отправляться на удаленный сервер системного журнала.
system syslog host <имя_узла> format <формат_сообщений>	Указание формата сообщений, в котором будут отправляться записи на удаленный сервер системного журнала.
system syslog host <имя_узла> port	Указание номера порта удаленного сервера системного журнала, по которому будут приниматься сообщения.
system syslog host <имя_узла> protocol <протокол>	Указание стандарта протокола, который будет использоваться для шифрования сообщений перед их отправкой на удаленный сервер системного журнала.
system syslog host <имя_узла> transport	Указание транспортного протокола, который будут использоваться

Команды настройки	
<протокол>	для отправления сообщений на удаленный сервер системного журнала.
system syslog mail-to <адрес_почты> facility <источник> level <уровень>	Указание типов сообщений, которые будут отправляться по электронной почте.
system syslog mail-to <адрес_почты> facility <источник> level <уровень> match <шаблон>	Выборка сообщений, которые будут отправляться по электронной почте, на основе указанного шаблона.
system syslog mail-to <адрес_почты> facility <источник> level <уровень> program <программа>	Указание типов сообщений, которые будут отправляться по электронной почте.
system syslog mail-to <адрес_почты> carbon-copy <адрес_почты>	Указание адреса электронной почты, на который будет отправляться копия сообщений.
system syslog mail-to <адрес_почты> mail-per-hour <количество>	Указание частоты отправки сообщений в час.
system mail smarthost <почтовый_шлюз>	Указание IP-адреса или символьного имени почтового шлюза.
system mail smarthost <почтовый_шлюз> auth-name <имя_пользователя>	Указание имени пользователя, используемого для аутентификации на указанном почтовом шлюзе.
system mail smarthost <почтовый_шлюз> auth-password <пароль>	Указание пароля, используемого для аутентификации на указанном почтовом шлюзе.
system mail smarthost <почтовый_шлюз> from <адрес_отправителя>	Указание адреса отправителя, который будет использоваться для данного почтового шлюза.
system mail smarthost <почтовый_шлюз> port <порт>	Указание порта для подключения к указанному почтовому шлюзу.
system mail tls-mode <режим>	Метод установления защищенного соединения с почтовым сервером.
system syslog host <имя_узла> x509-cert <сертификат>	Установка сертификата X.509 (сертификата SSL) в качестве дополнительного фактора аутентификации на почтовом сервере.
Эксплуатационные команды	
show log	Отображение системного журнала
dump log	Выгрузка записей системного журнала
clear log	Очистка записей системного журнала

9.2.1 system syslog

Настройка служебной программы системного журнала в системе.

Синтаксис

```
set system syslog
delete system syslog
show system syslog
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    syslog {
    }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для настройки служебной программы syslogd в системе.

При помощи этой команды можно установить места назначения для сообщений журнала от различных компонентов маршрутизации (источников) и указать минимальный уровень серьезности регистрируемых сообщений для каждого источника.

По умолчанию используется протокол надежной доставки сообщений согласно спецификации RFC 3195. По умолчанию сообщения передаются через порт номер 601 по протоколу TCP.

Сообщения журналов, созданные системой Numa Edge, связываются с одним из уровней серьёзности перечисленных в таблице уровней серьёзности. Numa Edge поддерживает стандартные типы источников сообщений системного журнала перечисленные в таблице источников сообщений системного журнала.

Форма **set** этой команды используется для создания узла конфигурации настроек системного журнала.

Формы **delete** этой команды используется для удаления настроек системного журнала.

Форма **show** этой команды может использоваться для просмотра настройки системного журнала.

9.2.2 system syslog console facility <источник> level <уровень>

Указание типов сообщений, отправляемых на консоль.

Синтаксис

```
set system syslog console facility <источник> [level <уровень>]
delete system syslog console facility [<источник> [level]]
show system syslog console facility [<источник> [level]]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   syslog {
      console {
         facility источник {
            level уровень
         }
      }
   }
}
```

Параметры

источник

Множественный узел. Типы сообщений, которые будут отправляться на консоль. Поддерживаемые типы источников сообщений приведены в таблице типов источников сообщений. Можно отправлять на консоль сообщения из нескольких типов источников, создав несколько узлов конфигурации facility в узле console.

уровень

Наименьший уровень серьезности для сообщения журнала, которое будет отправлено на консоль. Поддерживаются значения emerg, alert, crit, err, warning, notice, info и debug. Разъяснение смысла этих уровней приведено таблице уровней серьёзности сообщений.

Значение по умолчанию

Если не задавать наименьший уровень серьезности для сообщений журнала вручную, будет использоваться уровень **err**, соответствующий ошибкам в работе.

Указания по использованию

Эта команда используется для указания типов сообщений, которые будут отправляться на консоль.

ПРИМЕЧАНИЕ Под отправкой сообщений на консоль подразумевается вывод сообщений при подключении к системе с использованием serial-порта. При подключении по ssh сообщения, настроенные через **system syslog console** не отображаются.

Форма **set** этой команды используется для указания настроек вывода сообщений на консоль.

Форма **delete** этой команды используется для удаления настроек вывода сообщений на консоль.

Форма **show** этой команды может использоваться для просмотра настройки сообщений для консоли.

9.2.3 system syslog global max-age

Настройка времени жизни записей системного журнала в днях.

Синтаксис

```
set system syslog global max-age <дни>
delete system syslog global max-age
show system syslog global max-age
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   syslog {
      global {
         max-age дни {
         }
      }
   }
}
```

Параметры

дни

Устанавливает максимальный срок жизни записей в системном журнале. В качестве значения ожидается целое число.

Значение по умолчанию

По умолчанию время жизни записей в системном журнале не ограничено.

Указания по использованию

По умолчанию Numa Edge хранит все записи в системном журнале и запрещает его очистку без выгрузки записей. Данный атрибут меняет поведение системы, позволяя удалять старые записи вне зависимости от того были ли они выгружены или нет.

Факт удаления устаревших записей регистрируется в системном журнале.

```
2022-07-22 10:55:01 log-watch daemon notice 0 Удалены записи журнала старше 2 дней
```

В процессе работы по умолчанию сохраняются все данные, что может привести к занятию всего дискового пространства файлом системного журнала. Для очистки системного журнала в штатном режиме работы необходимо использовать команду выгрузки данных на внешний накопитель **dump log** либо настроить отправку сообщений журнала на удаленный сервер.

ПРИМЕЧАНИЕ Установка параметра max-age изменяет режим работы по умолчанию. Перед включением ротации рекомендуется настроить выгрузку системного журнала на сторонний сервер во избежание потери важных записей.

Форма **set** этой команды используется для указания максимального срока жизни записей в системном журнале.

Форма **delete** этой команды используется для удаления максимального срока жизни записей в системном журнале.

Форма **show** этой команды может использоваться для просмотра настройки максимального срока жизни записей в системном журнале.

9.2.4 system syslog global max-history

Настройка максимального количества записей в системном журнале, хранимых после выгрузки.

Синтаксис

```
set system syslog global max-history <количество_записей>
delete system syslog global max-history
show system syslog global max-history
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   syslog {
      global {
         max-history количество_записей {
         }
      }
   }
}
```

Параметры

количество_записей

Количество последних записей (строк), которые сохраняются в системе после ее выгрузки.

Значение по умолчанию

По умолчанию количество хранимых записей после выгрузки равно 10^6.

Указания по использованию

Этот атрибут используется для установки максимального количество последних записей, которые будут храниться в системном журнале после его выгрузки. Таким образом, данное значение не ограничивает общее количество записей в системном журнале, а ограничивает количество уже сохраненных.

О факте удаления выгруженных записей в системный журнал записывается сообщение, с уровнем серьезности **info**.

```
2022-07-22 16:30:02 log-watch daemon info   0 Удалены выгруженные записи журнала id <=
```

```
11561
```

Обратите внимание, что по умолчанию данная запись не попадает в системный журнал, поскольку уровень серьезности для всех событий установлено значение ***notice***.

Форма **set** этой команды используется для указания максимального количества выгруженных записей в системном журнале.

Форма **delete** этой команды используется для удаления максимального количества выгруженных записей в системном журнале.

Форма **show** этой команды может использоваться для просмотра максимального количества выгруженных записей в системном журнале.

9.2.5 system syslog global max-size

Настройка максимального занимаемого места на диске файлом системного журнала.

Синтаксис

```
set system syslog global max-size <размер>
delete system syslog global max-size
show system syslog global max-size
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   syslog {
      global {
         max-size размер {
         }
      }
   }
}
```

Параметры

размер

Размер системного журнала, указанный в мегабайтах (МБ). В качестве доступных значений ожидается целое число, однако необходимо иметь в виду, что для корректной работы данное значение не должно превышать размер раздела **/var/log**, в котором хранится системный журнал.

Значение по умолчанию

По умолчанию размер журнала не ограничен.

Указания по использованию

Этот атрибут используется для установки максимального размера занимаемого места на диске файлом системного журнала **/var/log/edge/system.db**. Определяется максимальное доступное пространство в мегабайтах.

В процессе работы по умолчанию сохраняются все данные, что может привести к занятию всего дискового пространства файлом системного журнала. Для очистки системного журнала в штатном режиме работы необходимо использовать команду выгрузки данных на внешний накопитель **dump log** либо настроить отправку сообщений журнала на удаленный сервер.

ПРИМЕЧАНИЕ Установка параметра max-size изменяет режим работы по умолчанию. Если системный журнал превышает значение, указанное данным параметром, то производится удаление 25% наименее актуальных записей системного журнала. Перед включением ротации рекомендуется настроить выгрузку системного журнала на сторонний сервер во избежание потери важных записей.

Форма **set** этой команды используется для указания максимального размера журнала.

Форма **delete** этой команды используется для удаления настройки максимального размера журнала.

Форма **show** этой команды может использоваться для просмотра настройки максимального размера журнала.

9.2.6 system syslog global signal-age

Настройка порогового значения срока жизни записей в системном журнале.

Синтаксис

```
set system syslog global signal-age <дни>
delete system syslog global signal-age
show system syslog global signal-age
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   syslog {
      global {
         signal-age дни {
         }
      }
   }
}
```

Параметры

дни

Устанавливает пороговое значение срока жизни записей в системном журнале. В качестве значения ожидается целое число.

Значение по умолчанию

По умолчанию пороговое значение времени жизни записей в системном журнале не ограничено.

Указания по использованию

Данный атрибут используется для задания порогового значения срока жизни записей в системном журнале. Если записи в системном журнале отличаются от системного времени на указанное количество дней, об этом будет произведена запись в системный журнал.

```
2022-07-21 19:30:01 log-watch daemon warnin 0 Записи журнала старше 1 дней
```

Форма **set** этой команды используется для задания порогового значения срока жизни записей в системном журнале.

Форма **delete** этой команды используется для удаления порогового значения срока жизни записей в системном журнале.

Форма **show** этой команды может использоваться для просмотра настройки максимального размера журнала.

9.2.7 system syslog global signal-rate

Установка интервала, используемого для регистрации сигнальных сообщений в системный журнал.

Синтаксис

```
set system syslog global signal-rate <часы>
delete system syslog global signal-rate
show system syslog global signal-rate
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   syslog {
      global {
         signal-rate часы {
         }
      }
   }
}
```

Параметры

часы

Устанавливает интервал в часах, который регулирует как часто будут сигнальные сообщения. Данные сообщения регистрируются в системном журнале после задания атрибутов signal-age и signal-max. В качестве значения ожидается целое число.

Значение по умолчанию

По умолчанию интервал регистрируемых сообщений равен 24 часам.

Указания по использованию

Сообщения о превышении порогового значения размера системного журнала (**signal-max**) и срока жизни записей (**signal-age**) по умолчанию регистрируются в системном журнале каждые 24 часа. Временем регистрации этих событий является время создания атрибута **system syslog global signal-rate**. Данный атрибут позволяет изменить частоту регистрации событий в часах.

Форма **set** этой команды используется для задания интервала регистрации сигнальных сообщений в системном журнале.

Форма **delete** этой команды используется для возврата интервала регистрации сигнальных сообщений в системном журнале на значение по умолчанию.

Форма **show** этой команды может использоваться для просмотра интервала регистрации сигнальных сообщений в системном журнале.

9.2.8 system syslog global signal-size

Настройка порогового значения занимаемого места на диске файлом системного журнала.

Синтаксис

```
set system syslog global signal-size <размер>
delete system syslog global signal-size
show system syslog global signal-size
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   syslog {
      global {
         signal-size размер {
         }
      }
   }
}
```

Параметры

дни

Устанавливает пороговое значение занимаемого места на диске файлом системного журнала в мегабайтах (МБ). В качестве значения ожидается целое число.

Значение по умолчанию

По умолчанию пороговое значение занимаемого места на диске файлом системного журнала не ограничено.

Указания по использованию

Данный атрибут используется для задания порогового значения занимаемого места на диске файлом системного журнала. Если объем файла системного журнала **/var/log/edge/system.db** превышает установленное значение, об этом будет произведена запись в системный журнал.

```
2022-07-21 19:30:01 log-watch daemon warnin 0 Записи журнала старше 1 дней
```

Форма **set** этой команды используется для задания порогового значения занимаемого места на диске файлом системного журнала.

Форма **delete** этой команды используется для удаления порогового значения занимаемого места на диске файлом системного журнала.

Форма **show** этой команды может использоваться для просмотра настройки порогового значения занимаемого места на диске файлом системного журнала.

9.2.9 system syslog global facility <источник> level <уровень>

Указание типов сообщений, которые будут отправляться в системный журнал.

Синтаксис

```
set system syslog global facility <источник> [level <уровень>]
delete system syslog global facility [<источник> [level]]
show system syslog global facility [<источник> [level]]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   syslog {
      global {
         facility источник {
            level уровень
         }
      }
```

```
    }
}
```

Параметры

источник

Множественный узел. Типы сообщений, которые будут отправляться в системный журнал. Поддерживаемые типы источников сообщений приведены в таблице типов источников сообщений. Можно отправлять в главный системный журнал сообщения из нескольких типов источников, создав несколько узлов конфигурации facility в узле конфигурации global.

уровень

Наименьший уровень серьёзности для сообщения журнала, которое будет записано. Поддерживаются значения emerg, alert, crit, err, warning, notice, info, debug. Разъяснение смысла этих уровней приведено в таблице уровней серьёзности.

Значение по умолчанию

Для всех источников регистрируются важные события (ntice), а для сообщений об авторизации — все события (all).

Указания по использованию

Эта команда используется для указания типов сообщений, которые будут отправляться в системный журнал.

Форма **set** этой команды используется для указания настроек для сообщений, отправляемых в системный журнал.

Форма **delete** этой команды используется для удаления настроек для сообщений, отправляемых в системный журнал.

Форма **show** этой команды может использоваться для просмотра настройки для сообщений, отправляемых в системный журнал.

9.2.10 system syslog host <имя_узла> address <адрес>

Указание адреса удаленного узла или доменного имени узла, куда отправляются сообщения журнала.

Синтаксис

```
set system syslog host <имя_узла> address <адрес>
delete system syslog host <имя_узла> address
show system syslog host <имя_узла> address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   syslog {
      host имя_узла {
         address адрес
      }
   }
}
```

Параметры

имя_узла

Множественный узел. Имя узла в системе конфигурирования Nume Edge, на который отправляются указанные сообщения журнала. На узле должна быть запущена служба **syslog**. В составе имени могут быть цифры, буквы и дефисы («-»).

адрес

В качестве значения для параметра адрес может быть указан IPv4-адрес или доменное имя узла, куда отправляются указанные сообщения журнала.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания адреса или доменного имени узла, на который будут отправляться указанные сообщения системного журнала.

Форма **set** этой команды используется для указания настроек адреса узла для отправки сообщений системного журнала.

Форма **delete** этой команды используется для удаления настроек адреса узла для отправки сообщений системного журнала.

Форма **show** этой команды может использоваться для просмотра настройки адреса узла для отправки сообщений системного журнала.

9.2.11 system syslog host <имя_узла> facility <источник> level <уровень>

Указание типов сообщений, которые будут отправляться на удаленный сервер системного журнала.

Синтаксис

```
set system syslog host <имя_узла> facility <источник> [level <уровень>]
delete system syslog host <имя_узла> facility [<источник> [level]]
show system syslog host <имя_узла> facility [<источник> [level]]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   syslog {
      host имя_узла {
         facility источник {
            level уровень
         }
      }
   }
}
```

Параметры

имя_узла

Множественный узел. Имя узла в системе конфигурирования Nume Edge, на который отправляются указанные сообщения журнала. На узле должна быть запущена служба syslog. В составе имени могут быть цифры, буквы и дефисы («-»). Можно отправлять сообщения журнала на несколько узлов, создав несколько узлов конфигурации host.

источник

Множественный узел. Типы сообщений, которые будут отправляться в главный системный журнал. Поддерживаемые типы источников сообщений приведены в таблице типов источников сообщений.

уровень

Наименьший уровень серьёзности для сообщения журнала, которое будет записано. Поддерживаются значения emerg, alert, crit, err, warning, notice, info, debug. Разъяснение смысла этих уровней приведено в таблице уровней серьёзности сообщений.

Значение по умолчанию

Если не задавать наименьший уровень серьезности для сообщений журнала вручную, будет использоваться уровень err, соответствующий ошибкам в работе.

Указания по использованию

Эта команда используется для указания типов сообщений, которые будут отправляться на удаленный сервер системного журнала.

Форма **set** этой команды используется для указания типов сообщений, которые будут отправляться на удаленный сервер системного журнала.

Форма **delete** этой команды используется для удаления настройки для сообщений, отправляемых на удаленный сервер системного журнала.

Форма **show** этой команды может использоваться для просмотра настройки для сообщений, отправляемых на удаленный сервер системного журнала.

9.2.12 system syslog host <имя_узла> format <формат_сообщений>

Указание формата, в котором сообщения будут отправляться на удаленный сервер системного журнала.

Синтаксис

```
set system syslog host <имя_узла> format <формат_сообщений>
delete system syslog host <имя_узла> format
show system syslog host <имя_узла> facility format
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   syslog {
      host имя_узла {
         format формат_сообщений
      }
   }
}
```

Параметры

имя_узла

Множественный узел. Имя узла в системе конфигурирования Nume Edge, на который отправляются указанные сообщения журнала. На узле должна быть запущена служба syslog. В составе имени могут быть цифры, буквы и дефисы («-»). Можно отправлять сообщения журнала на несколько узлов, создав несколько узлов конфигурации host.

формат_сообщений

Выбор формата, который будет использоваться для отправляемых сообщений. Допустимые значения представлены ниже:

plain: Текст без форматирования. Стандартный формат сообщения, используемый службой syslog;

cef: Формат Common Event Format.

Значение по умолчанию

По умолчанию используется формат **plain**.

Указания по использованию

Эта команда используется для указания типов сообщений, которые будут отправляться на удаленный сервер системного журнала.

Форма **set** этой команды используется для указания формата сообщений, отправляемых на удаленный сервер системного журнала.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** этой команды может использоваться для просмотра формата сообщений, отправляемых на удаленный сервер системного журнала.

9.2.13 system syslog host <имя_узла> port

Указание номера порта удаленного сервера системного журнала, по которому будут приниматься сообщения.

Синтаксис

```
set system syslog host <имя_узла> port [auto | <номер_порта>]
delete system syslog host <имя_узла> port
show system syslog host <имя_узла> port
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   syslog {
      host имя_узла {
         port auto|номер порта
         }
      }
   }
}
```

Параметры

имя_узла

Множественный узел. Имя узла в системе конфигурирования Nume Edge, на который отправляются указанные сообщения журнала. На узле должна быть запущена служба syslog. В составе имени могут быть цифры, буквы и дефисы («-»). Можно отправлять сообщения журнала на несколько узлов, создав несколько узлов конфигурации host.

номер_порта

Проверка соответствия по номеру порта. Значение должно лежать в диапазоне 1-65535.

auto

Используемый порт будет зависеть от сочетания протоколов прикладного и транспортного уровней. Допустимые сочетания представлены ниже:

IETF/TCP: 601;

IETF/UDP: 514;

IETF/TLS: 6514;

BSD/TCP: 514;

BSD/UDP: 514.

Значение по умолчанию

По умолчанию используется параметр **auto**.

Указания по использованию

Эта команда используется для указания номера порта удаленного сервера системного журнала, по которому будут приниматься сообщения.

Форма **set** этой команды используется для указания номера порта удаленного сервера системного журнала.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** этой команды может использоваться для просмотра порта удаленного сервера системного журнала.

9.2.14 system syslog host <имя_узла> protocol <протокол>

Указание стандарта протокола, который будет использоваться для шифрования сообщений перед их отправкой на удаленный сервер системного журнала.

Синтаксис

```
set system syslog host <имя_узла> protocol <протокол>
delete system syslog host <имя_узла> protocol
show system syslog host <имя_узла> protocol
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   syslog {
      host имя_узла {
         protocol протокол
      }
   }
}
```

Параметры

имя_узла

Множественный узел. Имя узла в системе конфигурирования Nume Edge, на который отправляются указанные сообщения журнала. На узле должна быть запущена служба syslog. В составе имени могут быть цифры, буквы и дефисы («-»). Можно отправлять сообщения журнала на несколько узлов, создав несколько узлов конфигурации host.

протокол

Выбор стандарта, который будет использоваться для шифрования отправляемых сообщений. Допустимые значения представлены ниже:

ietf: Отправляет сообщения в формате, описанном в RFC 5424;

bsd: Отправляет сообщения в формате, описанном в RFC 3164.

Значение по умолчанию

По умолчанию используется протокол **ietf**.

Указания по использованию

Эта команда используется для указания стандарта протокола, который будет использоваться для шифрования сообщений перед их отправкой на удаленный сервер системного журнала.

Форма **set** этой команды используется для указания протокола шифрования сообщений, отправляемых на удаленный сервер системного журнала.

Формы **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** этой команды может использоваться для просмотра протокола шифрования сообщений, отправляемых на удаленный сервер системного журнала.

9.2.15 system syslog host <имя_узла> transport <протокол>

Указание транспортного протокола, который будут использоваться для отправления сообщений на удаленный сервер системного журнала.

Синтаксис

```
set system syslog host <имя_узла> transport <протокол>
delete system syslog host <имя_узла> transport
show system syslog host <имя_узла> transport
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   syslog {
      host имя_узла {
         transport протокол
      }
   }
}
```

Параметры

имя_узла

Множественный узел. Имя узла в системе конфигурирования Nume Edge, на который отправляются указанные сообщения журнала. На узле должна быть запущена служба syslog. В составе имени могут быть цифры, буквы и дефисы («-»). Можно отправлять сообщения журнала на несколько узлов, создав несколько узлов конфигурации host.

протокол

Протокол транспортного уровня. Допустимые значения указаны ниже:

udp: выбор UDP протокола;

tcp: выбор TCP протокола;

tls: выбор TLS протокола (TCP, только для прикладного протокола IETF).

TLS возможен только в сочетании с протоколом IETF, при этом автоматически осуществляется аутентификация сервера по известным через модуль PKI сертификатам Удостоверяющего Центра.

Значение по умолчанию

По умолчанию в качестве протокола транспортного уровня используется **tcp**.

Указания по использованию

Эта команда используется для указания используемого транспортного протокола отправки сообщений на удаленный сервер системного журнала.

Форма **set** этой команды используется для указания транспортного протокола.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** этой команды может использоваться для просмотра используемого транспортного протокола отправки сообщений на удаленный сервер системного журнала.

9.2.16 system syslog mail-to <адрес_почты> facility <источник> level <уровень>

Указание типов сообщений, которые будут отправляться по электронной почте.

Синтаксис

```
set system syslog mail-to <адрес_почты> facility <источник> [level <уровень>]
delete system syslog mail-to <адрес_почты> facility [<источник> [level]]
show system syslog mail-to <адрес_почты> facility [<источник> [level]]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    syslog {
        mail-to адрес_почты {
            facility источник {
                level уровень
            }
        }
    }
}
```

Параметры

адрес_почты

Множественный узел. Адрес электронной почты получателя, на который будут отправляться указанные сообщения журнала.

источник

Множественный узел. Типы сообщений, которые будут отправляться в системный журнал. Поддерживаемые типы источников сообщений приведены в таблице типов источников сообщений.

уровень

Наименьший уровень серьёзности для сообщения журнала, которое будет записано. Поддерживаются значения emerg, alert, crit, err, warning, notice, info, debug. Разъяснение смысла этих уровней приведено в таблице уровней серьёзности.

Значение по умолчанию

Если не задавать наименьший уровень серьезности для сообщений журнала вручную, будет использоваться уровень **err**, соответствующий ошибкам в работе.

Указания по использованию

Эта команда используется для указания типов сообщений, которые будут отправляться на указанную электронную почту. Настройки подключения к почтовому шлюзу задаются при помощи ветви конфигурации **service mail smarthost**.

Форма **set** этой команды используется для указания типов сообщений, которые будут отправляться по электронной почте.

Форма **delete** этой команды используется для удаления типов сообщений, которые будут отправляться по электронной почте.

Форма **show** этой команды может использоваться для просмотра конфигурации.

9.2.17 system syslog mail-to <адрес_почты> facility <источник> level <уровень> match <шаблон>

Выборка сообщений, которые будут отправляться по электронной почте, на основе указанного шаблона.

Синтаксис

```
set system syslog mail-to <адрес_почты> facility <источник> level <уровень> match <шаблон>

delete system syslog mail-to <адрес_почты> facility [<источник> level <уровень> [match <шаблон>]]

show system syslog mail-to <адрес_почты> facility [<источник> [level <уровень> [match]]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    syslog {
        mail-to адрес_почты {
            facility источник {
                level уровень {
                    match шаблон
                }
            }
        }
    }
}
```

Параметры

адрес_почты

Множественный узел. Адрес электронной почты получателя, на который будут отправляться указанные сообщения журнала.

источник

Множественный узел. Типы сообщений, которые будут отправляться в системный журнал. Поддерживаемые типы источников сообщений приведены в таблице типов источников сообщений.

уровень

Наименьший уровень серьёзности для сообщения журнала, которое будет записано. Поддерживаются значения emerg, alert, crit, err, warning, notice, info, debug. Разъяснение смысла этих уровней приведено в таблице уровней серьёзности.

шаблон

Множественный узел. Шаблон для выборки сообщений системного журнала.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания шаблона, на основе которого осуществляется выборка сообщений, которые будут отправляться по указанному адресу электронной почты. В том случае если указаны несколько шаблонов для поиска, то соответствие будет установлено при нахождении хотя бы для одного из них.

Форма **set** этой команды используется для указания шаблона, на основе которого осуществляется выборка сообщений для отправки.

Форма **delete** этой команды используется для удаления шаблона, на основе которого осуществляется выборка сообщений для отправки.

Форма **show** этой команды может использоваться для просмотра шаблонов, на основе которых осуществляется выборка сообщений для отправки.

9.2.18 system syslog mail-to <адрес_почты> facility <источник> level <уровень> program <программа>

Выборка сообщений, которые будут отправляться по электронной почте, на основе указанной исполняемой программы или системной службы.

Синтаксис

```
set system syslog mail-to <адрес_почты> facility <источник> level <уровень> program <программа>

delete system syslog mail-to <адрес_почты> facility [<источник> level <уровень> [program <программа>]]

show system syslog mail-to <адрес_почты> facility [<источник> [level <уровень> [program]]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    syslog {
        mail-to адрес_почты {
            facility источник {
                level уровень {
                    program программа
                }
            }
        }
    }
}
```

Параметры

адрес_почты

Множественный узел. Адрес электронной почты получателя, на который будут отправляться указанные сообщения журнала.

источник

Множественный узел. Типы сообщений, которые будут отправляться в системный журнал. Поддерживаемые типы источников сообщений приведены в таблице типов источников сообщений.

уровень

Наименьший уровень серьёзности для сообщения журнала, которое будет записано. Поддерживаются значения emerg, alert, crit, err, warning, notice, info, debug. Разъяснение смысла этих уровней приведено в таблице уровней серьёзности.

программа

Множественный узел. Имя программы или системной службы, для которой приводится выборка сообщений.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отправки на указанную электронную почту сообщений, отставленных определенной программой или системной службой.

Форма **set** этой команды используется для указания выборки сообщений для отправки на указанную электронную почту основываясь на исполняемой программе или системной службе.

Форма **delete** этой команды используется для удаления выборки сообщений для отправки на указанную электронную почту основываясь на исполняемой программе или системной службе.

Форма **show** этой команды может использоваться для просмотра конфигурации.

9.2.19 system syslog mail-to <адрес_почты> carbon-copy <адрес_почты>

Указание адреса электронной почты, на который будет отправляться копия сообщений.

Синтаксис

```
set system syslog mail-to <адрес_почты> carbon-copy <адрес_почты>
delete system syslog mail-to <адрес_почты> carbon-copy <адрес_почты>
show system syslog mail-to <адрес_почты> carbon-copy <адрес_почты>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   syslog {
      mail-to адрес_почты {
         carbon-copy адрес_почты
      }
   }
}
```

Параметры

mail-to *адрес_почты*

Множественный узел. Адрес электронной почты получателя, на который будут отправляться указанные сообщения журнала.

carbon-copy *адрес_почты*

Множественный узел. Адрес электронной почты получателя, на который будут отправляться копии сообщений.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания адреса электронной почты, на который будут отправляться копии сообщений.

Формы **set** этой команды используется для указания адреса электронной почты, на который будут отправляться копии сообщений.

Форма **delete** этой команды используется для удаления адреса электронной почты, на который будут отправляться копии сообщений.

Форма **show** этой команды может использоваться для просмотра адресов электронной почты, на который будут отправляться копии сообщений.

9.2.20 system syslog mail-to <адрес_почты> mail-per-hour <количество>

Указание частоты отправки сообщений в час.

Синтаксис

```
set system syslog mail-to <адрес_почты> mail-per-hour <количество>
```

```
delete system syslog mail-to <адрес_почты> mail-per-hour
show system syslog mail-to <адрес_почты> mail-per-hour
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   syslog {
      mail-to адрес_почты {
         mail-per-hour количество
      }
   }
}
```

Параметры

адрес_почты

Множественный узел. Адрес электронной почты получателя, на который будут отправляться указанные сообщения журнала.

количество

Максимальное количество сообщений, которое может быть отправлено в час. Значение должно лежать в диапазоне от 1 до 60.

Значение по умолчанию

По умолчанию отправляется 6 сообщений в час.

Указания по использованию

Эта команда используется для указания количества сообщений в час, которые будут отправляться на указанный адрес электронной почты.

Форма **set** этой команды используется для указания количества сообщений в час, которые будут отправляться на указанный адрес электронной почты.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** этой команды используется для просмотра количества сообщений в час, которые будут отправляться на указанный адрес электронной почты.

9.2.21 system mail smarthost <почтовый_шлюз>

Указание IP-адреса или символьного имени почтового шлюза.

Синтаксис

```
set system mail smarthost <почтовый_шлюз>
delete service mail smarthost <почтовый_шлюз>
show service mail smarthost <почтовый_шлюз>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   mail smarthost почтовый_шлюз {
   }
}
```

Параметры

почтовый_шлюз

Доменное имя, IPv4-адрес или IPv6-адрес почтового шлюза, используемого для пересылки писем.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда позволяет указать доменное имя или адрес почтового шлюза, который будет использован для пересылки писем.

ПРИМЕЧАНИЕ В системе конфигурации Numa Edge одновременно может быть настроен только один почтовый шлюз.

ОБРАТИТЕ ВНИМАНИЕ Текущая версия системы Numa Edge не имеет возможности настройки почтового шлюза с использованием шифрования!

Форма **set** этой команды используется для указания почтового шлюза.

Форма **delete** этой команды используется для удаления настроенного почтового шлюза.

Форма **show** этой команды используется для просмотра настроек почтового шлюза.

9.2.22 system mail smarthost <почтовый_шлюз> auth-name <имя_пользователя>

Указание имени пользователя, используемого для аутентификации на указанном почтовом шлюзе.

Синтаксис

```
set system mail smarthost <почтовый_шлюз>  auth-name <имя_пользователя>
delete system mail smarthost <почтовый_шлюз>  auth-name
show system mail smarthost <почтовый_шлюз> auth-name
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   mail {
      smarthost почтовый шлюз {
         auth-name имя_пользователя
      }
   }
}
```

Параметры

почтовый_шлюз

Доменное имя, IPv4-адрес или IPv6-адрес почтового шлюза, используемого для пересылки писем.

имя_пользователя

Имя пользователя, используемое для аутентификации на указанном почтовом шлюзе.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда позволяет при необходимости указать имя пользователя, которое будет использовано для аутентификации на указанном почтовом шлюзе.

Форма **set** этой команды используется для указания имени пользователя, используемого для аутентификации на почтовом шлюзе.

Форма **delete** этой команды используется для удаления имени пользователя, используемого для аутентификации на почтовом шлюзе.

Форма **show** этой команды используется для просмотра имени пользователя, используемого для аутентификации на почтовом шлюзе.

9.2.23 system mail smarthost <почтовый_шлюз> auth-password <пароль>

Указание пароля, используемого для аутентификации на указанном почтовом шлюзе.

Синтаксис

```
set system mail smarthost <почтовый_шлюз> auth-password <пароль>
delete system mail smarthost <почтовый_шлюз> auth-password
show system mail smarthost <почтовый_шлюз> auth-password
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   mail {
      smarthost почтовый_шлюз {
         auth-password пароль
      }
   }
}
```

Параметры

почтовый_шлюз

Доменное имя, IPv4-адрес или IPv6-адрес почтового шлюза, используемого для пересылки писем.

пароль

Пароль, используемый для аутентификации на указанном почтовом шлюзе.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда позволяет при необходимости указать пароль, который будет использован для аутентификации на указанном почтовом шлюзе.

Форма **set** этой команды используется для указания пароля пользователя, используемого для аутентификации на почтовом шлюзе.

Форма **delete** этой команды используется для удаления пароля пользователя, используемого для аутентификации на почтовом шлюзе.

Форма **show** этой команды используется для просмотра пароля пользователя, используемого для аутентификации на почтовом шлюзе.

9.2.24 system mail smarthost <почтовый_шлюз> from <адрес_отправителя>

Указание адреса отправителя, который будет использоваться для данного почтового шлюза.

Синтаксис

```
set system mail smarthost <почтовый_шлюз> from <адрес_отправителя>
delete system mail smarthost <почтовый_шлюз> from
show system mail smarthost <почтовый_шлюз> from
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   mail {
      smarthost почтовый_шлюз {
         from адрес_отправителя
      }
   }
}
```

Параметры

почтовый_шлюз

Доменное имя, IPv4-адрес или IPv6-адрес почтового шлюза, используемого для пересылки писем.

адрес_отправителя

Адрес отправителя. Указывается значение, которое будет помещено в поле 'From' отправляемого сообщения. Допустимые форматы представлены ниже:

<имя_пользователя>@<имя_узла>;

<имя_пользователя> (при этом в качестве <имени_узла> будет добавлено имя оборудования и домен).

Значение по умолчанию

По умолчанию в качестве адреса отправителя используется конструкция **<имя_пользователя>@<имя_узла>**, где имя пользователя – **root**, а имя узла представляет собой имя оборудования и домен.

Указания по использованию

Эта команда используется для указания адреса отправителя. Почтовый шлюз будет пересылать письма указывая в качестве адреса отправителя установленное значение.

Форма **set** этой команды используется для указания адреса отправителя.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** этой команды используется для просмотра адреса отправителя.

9.2.25 system mail smarthost <почтовый_шлюз> port <порт>

Указание порта, используемого для подключения к указанному почтовому шлюзу.

Синтаксис

```
set system mail smarthost <почтовый_шлюз> port <порт>
delete system mail smarthost <почтовый_шлюз> port
show system mail smarthost <почтовый_шлюз> port
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
```

```
    mail {
        smarthost почтовый_шлюз {
            port порт
        }
    }
}
```

Параметры

почтовый_шлюз

Доменное имя, IPv4-адрес или IPv6-адрес почтового шлюза, используемого для пересылки писем.

порт

Порт, используемый для подключения к указанному почтовому шлюзу. Допустимые значения представлены в таблице ниже.

Таблица 29 – Допустимые форматы указания порта

Значение	Описание
Text	Имя порта (любое из файла /etc/services).
1-65535	Номер порта.

Значение по умолчанию

По умолчанию используется порт 25.

Указания по использованию

Эта команда позволяет указать порт, который используется для подключения к указанному почтовому шлюзу.

Форма **set** этой команды используется для указания порта для подключения к почтовому шлюзу.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** этой команды используется для просмотра порта для подключения к почтовому шлюзу.

9.2.26 system mail tls-mode <режим>

Режим установления защищенного соединения с почтовым сервером.

Синтаксис

```
set system mail tls-mode <режим>
delete service mail tls-mode
show service mail tls-mode
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    mail {
        tls-mode режим
    }
}
```

Параметры

режим

Данный параметр определяет режим установки соединения с почтовым сервером. Допустимые значения указаны ниже:

disabled: Соединение без SSL/TLS;

smtps: SSL/TLS соединение с использованием SMTPS;

starttls: SSL/TLS соединение с использованием STARTTLS;

Значение по умолчанию

По умолчанию соединение с почтовым сервером устанавливается без использования SSL/TLS, значение **disabled**.

Указания по использованию

Эта команда позволяет указать режим установки соединения с почтовым сервером.

ПРИМЕЧАНИЕ В системе конфигурации Numa Edge одновременно может быть настроен только один почтовый шлюз.

Форма **set** этой команды используется для указания почтового шлюза.

Форма **delete** этой команды используется для удаления настроенного почтового шлюза.

Форма **show** этой команды используется для просмотра настроек почтового шлюза.

9.2.27 system syslog host <имя_узла> x509-cert <сертификат>

Установка сертификата X.509 (сертификата SSL) в качестве дополнительного фактора аутентификации на почтовом сервере.

Синтаксис

```
set system mail x509-cert <сертификат>
delete system mail x509-cert
show system mail x509-cert
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   mail {
         x509-cert сертификат
      }
   }
```

Параметры

сертификат
Клиентский сертификат X.509, используемый в качестве дополнительного фактора аутентификации на почтовом сервере.

Значение по умолчанию

Отсутствует.

Указания по использованию

Если при установлении TLS соединения, сервер запрашивает клиентский сертификат и данный параметр настроен, то сертификат будет передан на сервер. Если сервер не запрашивает клиентский сертификат, вне зависимости от значений данного параметра, сертификат на сервер не передается.

ПРИМЕЧАНИЕ Клиентский сертификат указывается среди доступных сертификатов блока конфигурации **pki**.

Форма **set** этой команды используется для указания клиентского сертификата X.509 при отправке сообщений на удаленный сервер системного журнала.

Форма **delete** этой команды используется для указания клиентского сертификата X.509 при отправке сообщений на удаленный сервер системного журнала.

Форма **show** этой команды может использоваться для просмотра используемого клиентского сертификата X.509 при отправке сообщений на удаленный сервер системного журнала.

9.2.28 show log

Отображение системного журнала.

Синтаксис

```
show log [authorization | date <дата> | from-date <дата> [to-date <дата>] | from-level <уровень> | program <программа> | programs | tail [<количество_сообщений>] | to-date <дата>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

authorization

Отображения сообщений, относящихся к авторизации из системного журнала (к объекту "auth").

date *дата*

Отображение сообщений системного журнала за определённую дату. Дата или время отображаемых сообщений журнала задаются в формате **'ГГГГ.ММ.ДД [чч[:мм[:сс]]]'**. В качестве даты можно задать только время, в этом случае будет производиться выборка за текущий день по указанному времени.

from-date *дата*

Отображение сообщений системного журнала начиная от указанной даты. Если параметр to-date не задан, то отображаются сообщения по текущую дату, если задан, то до даты указанной в параметре to-date. Дата или время отображаемых сообщений журнала задаются в формате **'ГГГГ.ММ.ДД [чч[:мм[:сс]]]'**. В качестве даты можно задать только время, в этом случае будет производиться выборка с указанного времени за текущий день.

from-level *уровень*

Отображение сообщений системного журнала, соответствующих указанному уровню критичности и выше.

program программа

Отображение сообщений системного журнала, оставленных определённой программой/службой.

programs

Отображение списка программ/служб, сообщения которых хранятся в системном журнале.

tail

Отображение последних строк системного журнала. При использовании команды без параметров отображаются последние десять строк.

количество_сообщений

Отображение указанного количество последних строк сообщений системного журнала.

to-date *дата*

Отображение сообщений системного журнала до указанной даты. Дата или время отображаемых сообщений журнала задаются в формате **'ГГГГ.ММ.ДД [чч[:мм[:сс]]]'**. В качестве даты можно задать только время, в этом случае будет производиться выборка до указанного времени текущего дня.

Указания по использованию

Эта команда используется для вывода сообщений системного журнала. По умолчанию при использовании без аргументов выводятся все сообщения системного журнала, отсортированные по времени начиная с самых старых сообщений.

Примеры

В примере ниже выводятся 10 последних сообщений системного журнала.

Пример 91– Отображение 10 последних сообщений системного журнала.

```
admin@edge:~$ show log tail
Дата       Время    Программа Объект Уров.  E Сообщение
2018-10-10 09:00:03 selftest  user   notice 0 Тест фильтрации: успешно
2018-10-10 09:00:03 selftest  user   notice 0 Тест работы механизмов контроля
целостности: успешно
2018-10-10 09:00:03 selftest  user   notice 0 Проверка записи в журнал
2018-10-10 09:00:03 selftest  user   notice 0 Тест регистрации действий:
успешно
2018-10-10 09:00:04 selftest  user   notice 0 Тест аутентификации: успешно
2018-10-10 10:00:02 selftest  user   notice 0 Тест фильтрации: успешно
2018-10-10 10:00:02 selftest  user   notice 0 Тест работы механизмов контроля
целостности: успешно
2018-10-10 10:00:02 selftest  user   notice 0 Проверка записи в журнал
2018-10-10 10:00:02 selftest  user   notice 0 Тест регистрации действий:
успешно
2018-10-10 10:00:04 selftest  user   notice 0 Тест аутентификации: успешно
admin@edge:~$
```

В примере ниже выводятся сообщения системного журнала, оставленные службой sshd.

Пример 92– Отображение сообщений системного журнала, оставленных службой sshd.

```
admin@edge:~$ show log program sshd
Дата       Время    Программа Объект Уров.  E Сообщение
2018-10-10 09:51:28 sshd      daemon notice 0 Starting service
2018-10-10 10:02:19 sshd      auth   info   0 Accepted keyboard-
interactive/pam for admin from 192.168.10.4 port 47134 ssh2
2018-10-10 10:06:26 sshd      auth   info   0 Received signal 15; terminating.
2018-10-10 10:07:15 sshd      auth   info   0 Server listening on 0.0.0.0 port
22.
2018-10-10 10:08:37 sshd      auth   info   0 Accepted keyboard-
interactive/pam for admin from 192.168.10.4 port 47168 ssh2
admin@edge:~$
```

Возможные ошибки

В редких случаях журнал регистрации событий может быть недоступен для просмотра при активном процессе записи событий в журнал. Пример недоступности журнала приведен ниже.

```
admin@edge:~$ show log tail 20
Ошибка базы данных журналирования: database is locked
```

В данном случае, для просмотра журнала регистрации событий следует обратиться к нему позже.

9.2.29 dump log

Выгрузка системного журнала

Синтаксис

`dump log [all | date <дата> | from-date <дата> [to-date <дата>] | to-date <дата>] to <имя_файла>`

Режим интерфейса

Эксплуатационный режим.

Параметры

all

Выгрузка всех сообщений системного журнала.

date *дата*

Выгрузка сообщений системного журнала за определённую дату. Дата или время отображаемых сообщений журнала задаются в формате **'ГГГГ.ММ.ДД [чч[:мм[:сс]]]'**. В качестве даты можно задать только время, в этом случае будет производиться выборка за текущий день по указанному времени.

from-date *дата*

Выгрузка сообщений системного журнала начиная от указанной даты. Если параметр to-date не задан, то выгружаются сообщения по текущую дату, если задан, то до даты указанной в параметре to-date. Дата или время выгружаемых сообщений журнала задаются в формате **'ГГГГ.ММ.ДД [чч[:мм[:сс]]]'**. В качестве даты можно задать только время, в этом случае будет производиться выборка с указанного времени за текущий день.

to-date *дата*

Выгрузка сообщений системного журнала до указанной даты. Дата или время отображаемых сообщений журнала задаются в формате **'ГГГГ.ММ.ДД [чч[:мм[:сс]]]'**. В качестве даты можно задать только время, в этом случае будет производиться выборка до указанного времени текущего дня.

имя_файла

Имя файла системного журнала, включая полный путь к его местонахождению.

Указания по использованию

Эта команда используется для выгрузки сообщений системного журнала. В последствии, выгруженные записи в системе Numa Edge можно удалить используя команду **clear log**.

Системный журнал можно выгрузить локально, на внешний носитель (подключенный по USB), на сервер TFTP, на сервер FTP, на сервер SCP или на сервер HTTP. Каталогом по умолчанию является /home/admin/.

В приведенной ниже таблице показан синтаксис указания выгружаемого файла системного журнала для различных местоположений файла.

Таблица 30 – Способы указания местоположения для выгружаемого файла системного журнала

Местоположение	Способ указания
Абсолютный путь	Используется стандартный способ указания файла в UNIX.
Относительный путь	Указывается имя файла с путем относительно каталога конфигурации по умолчанию.
Сервер FTP	Используется следующий синтаксис для параметра *имя_файла:* **ftp:**//*пользователь @узел/файл_системного_журнала*, где *пользователь* - это имя пользователя на узле, *узел* - это имя узла или IP-адрес сервера FTP, а *файл_системного_журнала* - это выгружаемый файл, включая путь. Если пользователь не указан, будет выдан запрос на ввод.
Сервер SCP	Используется следующий синтаксис для параметра *имя_файла:* **scp:**//*пользователь@узел/файл_системного_журнала*, где *пользователь* - это имя пользователя на узле, *узел* - это имя узла или IP-адрес сервера SCP, а *файл_системного_журнала*- это выгружаемый файл, включая путь. Если пользователь не указан, будет выдан запрос на ввод.
Сервер HTTP	Используется следующий синтаксис для параметра *имя_файла*: **http**://*узел/файл_системного_журнала*, где *узел* - это имя узла или IP-адрес сервера HTTP, а *файл_системного_журнала* - это файл выгрузки журнала, включая путь.
Сервер TFTP	Используется следующий синтаксис для параметра *имя_файла*: **tftp:**//*узел/файл_системного_журнала*, где *узел* - это имя узла или IP-адрес сервера TFTP, а *файл_системного_журнала* - это файл выгрузки журнала, включая путь относительно корневого каталога TFTP.

9.2.30 clear log

Отображение системного журнала

Синтаксис

```
clear log
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Указания по использованию

Эта команда используется для очистки сообщений системного журнала.

ПРИМЕЧАНИЕ В режиме работы системного журнала по умолчанию запрещена очистка сообщений системного журнала без их предварительной выгрузки. Чтобы иметь возможность очистки сообщений системного журнала без их предварительной выгрузки необходимо установить параметр **system syslog global max-size**.

10 Настройка интерфейсов

10.1 Управляющий интерфейс

В данном разделе описаны следующие команды.

Таблица 31 – Команды настройки управляющего интерфейса Numa Edge

Эксплуатационные команды	
system management <состояние>	Включение/выключение управляющего интерфейса Numa Edge.

10.1.1 system management <состояние>

Включение/выключение управляющего интерфейса Numa Edge.

Синтаксис

```
system management <состояние>
system management on
system management off
```

Режим интерфейса

Эксплуатационный режим.

Параметры

состояние

Указание включения/выключения управляющего интерфейса Numa Edge. Допустимые значения представлены ниже:

on: включение управляющего интерфейса.

off: выключение управляющего интерфейса.

Указания по использованию

ПРЕДУПРЕЖДЕНИЕ При ошибке в конфигурации возможна потеря сетевого доступа к системе.

Изменение данного параметра влечёт за собой автоматическое сохранение конфигурации во время фиксации.

Команда используется для включения и выключения управляющего интерфейса Numa Edge. По умолчанию, первый из интерфейсов платформы имеет имя **ethm** и недоступен для штатных средств конфигурации. При этом, на нём всегда настроен адрес 192.168.200.1/24 и работают службы DHCP, SSH и HTTPS, что позволяет использовать его для конфигурации МЭ при любых ошибках в конфигурации других интерфейсов и служб.

В случае необходимости, при конфликте настроенного штатного диапазона адресов подсети **ethm** с другими сетями или при желании использовать все доступные интерфейсы МЭ для работы в обслуживаемых сетях, данная команда позволяет отключить такое поведение управляющего интерфейса.

ПРИМЕЧАНИЕ
Переключение управляющего интерфейса не является повседневной операцией.

- Переключение управляющего интерфейса рекомендуется выполнять во временные промежутки, предназначенные для выполнения соответствующих технических работ.
- Переключение управляющего интерфейса вызывает перезапуск всех сервисов Изделия, что может привести к перерыву в обслуживании.
- Несмотря на то, что перезагрузка Изделия после после переключения управляющего интерфейса в общем случае не требуется - рекомендуется ее выполнить.
- Перед переключением настоятельно рекомендуется проверить наличие и актуальность полной резервной копии конфигурации Изделия.

При выключении управляющего интерфейса (выполнении команды **system management off**) происходит переименование интерфейса **ethm** в **eth0** (в зависимости от аппаратной платформы имя интерфейса может

различаться, например быть **eth1** или **eth-a0**) и прописывание всех настроенных на нём служб в конфигурацию МЭ. При этом интерфейсом **eth0** можно будет пользоваться так же, как и любым другим.

При обратном переключении (выполнении команды **system management on**) происходит переименование первого интерфейса платформы (как правило **eth0)** в **ethm** и на интерфейсе **ethm** запускаются штатные для него службы DHCP, SSH и HTTPS.

10.2 Настройка интерфейсов Ethernet

В данном разделе описаны следующие команды.

Таблица 32 – Команды настройки интерфейсов Ethernet

Команды настройки	
interfaces ethernet <ethx>	Определение интерфейса Ethernet.
interface ethernet <ethx> address	Назначение IP-адреса и префикса сети интерфейсу Ethernet.
interfaces ethernet <ethx> description <описание>	Текстовое описание интерфейса Ethernet.
interfaces ethernet <ethx> disable	Отключение интерфейса Ethernet с сохранением настройки.
interfaces ethernet <ethx> disable-flow-control	Отключение механизма контроля перегрузок для интерфейса Ethernet.
interfaces ethernet <ethx> duplex <режим_дуплекса>	Установка режима дуплекса для интерфейса Ethernet.
interfaces ethernet <ethx> enable-proxy-arp	Включение режима проксирования ARP для интерфейса Ethernet.
interfaces ethernet <ethx> lldp <режим>	Установка режима работы протокола LLDP на интерфейсе.
interfaces ethernet <ethx> mac <mac-адрес>	Назначение MAC-адреса для интерфейса Ethernet.
interfaces ethernet <ethx> mtu <mtu>	Установка значения MTU для интерфейса Ethernet.
interfaces ethernet <ethx> speed <скорость>	Установка скорости интерфейса Ethernet.
Эксплуатационные команды	
clear interfaces ethernet <ethx> counters	Очистка статистических счетчиков для интерфейса Ethernet.
show interfaces ethernet	Вывод сведений и статистических данных для интерфейсов Ethernet.

10.2.1 interfaces ethernet <ethx>

Определение интерфейса Ethernet.

Синтаксис

```
set interfaces ethernet <ethx>
delete interfaces ethernet <ethx>
show interfaces ethernet <ethx>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    ethernet ethx {
    }
}
```

Параметры

ethx

Множественный узел. Идентификатор для определяемого интерфейса Ethernet. Значение должно лежать в диапазоне от eth0 до eth999 в зависимости от реально имеющихся в системе интерфейсов Ethernet. Количество

созданных узлов конфигурации интерфейсов Ethernet совпадает с количеством физических сетевых интерфейсов Ethernet, установленных в системе.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для настройки интерфейсов Ethernet.

Форма **set** данной команды позволяет создать узел конфигурации интерфейса Ethernet, если интерфейс физически существует в системе.

ПРИМЕЧАНИЕ Чтобы вывести список всех физических интерфейсов, доступных ядру системы, следует использовать параметр **system** команды **show interfaces**.

Форма **delete** данной команды используется для удаления узла конфигурации соответствующего интерфейса Ethernet. При следующем запуске системы для интерфейса будет создан пустой узел конфигурации.

Форма **show** данной команды используется для отображения настройки интерфейса Ethernet.

10.2.2 interface ethernet <ethx> address

Назначение IP-адреса и префикса сети интерфейсу Ethernet.

Синтаксис

```
set interfaces ethernet <ethx> address [<ip-адрес> | dhcp]

delete interfaces ethernet <ethx> address [<ip-адрес> | dhcp]

show interfaces ethernet ethx address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      address ip-адрес | dhcp
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

ip-адрес

IPv4-адрес или IPv6-адрес для данного интерфейса Ethernet. Допустимые значения представлены в таблице ниже:

Таблица 33 – Формат указания ip-адреса для интерфейса

Значение	Описание
<x.x.x.x/x>	IPv4-адрес/префикс (например: 192.168.10.254/24).
<h:h:h:h:h:h:h:h/x>	IPv6-адрес/префикс (например, 2001:db8:1234::/48)

Назначить интерфейсу несколько IP-адресов можно, создав соответствующее количество узлов конфигурации **address.**

dhcp

Параметр определяет интерфейс как клиент протокола DHCP, получающий адрес и префикс от сервера DHCP.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для назначения IP-адреса и префикса сети интерфейсу Ethernet.

Если используется параметр **dhcp**, значение MTU также будет устанавливаться динамически за исключением случая, когда оно определяется явно с помощью команды **interfaces ethernet <ethx> mtu <mtu>**, которая имеет более высокий приоритет.

Форма **set** данной команды используется для назначения IP-адреса и сетевого префикса. Для назначения интерфейсу нескольких IP-адресов следует создать соответствующее количество узлов конфигурации **address.**

Форма **delete** данной команды используется для удаления настройки IP-адреса.

Форма **show** данной команды используется для отображения настройки IP-адреса.

10.2.3 interfaces ethernet <ethx> description <описание>

Текстовое описание интерфейса Ethernet.

Синтаксис

```
set interfaces ethernet <ethx> description <описание>
delete interfaces ethernet <ethx> description
show interfaces ethernet <ethx> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      description описание
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

описание

Мнемоническое имя или описание интерфейса Ethernet.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для установки текстового описания интерфейса Ethernet.

Форма **set** данной команды используется для установки описания.

Форма **delete** данной команды используется для удаления описания.

Форма **show** данной команды используется для отображения настройки описания.

10.2.4 interfaces ethernet <ethx> disable

Отключение интерфейса Ethernet с сохранением настройки.

Синтаксис

```
set interfaces ethernet <ethx> disable
delete interfaces ethernet <ethx> disable
```

```
show interfaces ethernet <ethx>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
     disable
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для отключения интерфейса Ethernet без удаления настройки.

Форма **set** данной команды используется для отключения интерфейса.

Форма **delete** данной команды используется для включения интерфейса.

Форма **show** данной команды используется для отображения настройки интерфейса Ethernet.

10.2.5 interfaces ethernet <ethx> disable-flow-control

Отключение механизма контроля перегрузок для интерфейса Ethernet.

Синтаксис

```
set interfaces ethernet <ethx> disable-flow-control
delete interfaces ethernet <ethx> disable-flow-control
show interfaces ethernet <ethx>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      disable-flow-control
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для отключения механизма контроля и предотвращения перегрузок для указанного интерфейса Ethernet.

Форма **set** данной команды используется для отключения механизма контроля перегрузок для интерфейса.

Форма **delete** данной команды используется для включения механизма контроля перегрузок для интерфейса.

Форма **show** данной команды используется для отображения настройки интерфейса Ethernet.

10.2.6 interfaces ethernet <ethx> duplex <режим_дуплекса>

Установка режима дуплекса для интерфейса Ethernet.

Синтаксис

```
set interfaces ethernet <ethx> duplex <режим_дуплекса>

delete interfaces ethernet <ethx> duplex

show interfaces ethernet <ethx> duplex
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      duplex режим_дуплекса   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

режим_дуплекса

Режим дуплекса интерфейса. Допустимые значения представлены в таблице ниже:

Таблица 34 – Режимы дуплекса

Значение	Описание
auto	Маршрутизатор автоматически согласует режим дуплекса с интерфейсом на другом конце канала.
half	Полудуплексный режим.
full	Полнодуплексный режим.

Значение по умолчанию

Маршрутизатор автоматически согласует режим дуплекса.

Указания по использованию

Команда используется для установки характеристик режима дуплекса для интерфейса Ethernet. Если режим дуплекса устанавливается явно, то также потребуется явно указать значение параметра **interfaces ethernet ethx speed**.

ПРИМЕЧАНИЕ Не всё оборудование поддерживает возможность явного указания режима дуплекса (или определенные режимы работы). Если используется оборудование, не поддерживающее такую установку (или определенные режимы работы), при фиксации изменений будет отображено сообщение об ошибке.

Форма **set** данной команды используется для установки режима дуплекса интерфейса Ethernet.

Форма **delete** данной команды используется для восстановления поведения, принятого по умолчанию.

Форма **show** данной команды используется для просмотра настройки режима дуплекса интерфейса Ethernet.

10.2.7 interfaces ethernet <ethx> enable-proxy-arp

Включение режима проксирования ARP для интерфейса Ethernet.

Синтаксис

```
set interfaces ethernet <ethx> enable-proxy-arp

delete interfaces ethernet <ethx> enable-proxy-arp

show interfaces ethernet <ethx>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      enable-proxy-arp
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

Значение по умолчанию

Режим проксирования ARP для интерфейса Ethernet отключен.

Указания по использованию

Команда используется для включения режима проксирования ARP (Address Resolution Protocol) для интерфейса Ethernet.

Режим проксирования ARP позволяет интерфейсу Ethernet отвечать на запросы ARP (используя свой собственный MAC-адрес) в том случае, если IP-адрес назначения принадлежит подсетям, подключенным к другим интерфейсам системы. Последующие пакеты для данного IP-адреса назначения будут соответствующим образом перенаправляться системой.

Форма **set** данной команды используется для включения режима проксирования ARP для интерфейса Ethernet.

Форма **delete** данной команды используется для восстановления поведения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки.

10.2.1 interfaces ethernet <ethx> lldp <режим>

Изменение режима работы протокола LLDP на указанном интерфейсе.

Синтаксис

```
set interfaces ethernet <ethx> lldp <режим>

delete interfaces ethernet <ethx> lldp

show interfaces ethernet <ethx> lldp
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      lldp режим
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

lldp

Режим работы протокола LLDP на указанном интерфейсе. Доступны следующие значения:

Таблица 35 – режимы работы LLDP

Значение	Описание
on	Включает прием и передачу LLDP сообщений.
tx	Включает только передачу LLDP сообщений.
rx	Включает только прием LLDP сообщений.
off	Отключает LDDP на указанном интерфейсе. Режим работы по умолчанию на всех интерфейсах, кроме ethm.

Значение по умолчанию

По умолчанию lldp выключен на всех интерфейсах **off**, кроме управляющего интерфейса (**ethm**).

Указания по использованию

Команда используется для изменения режима работы протокола LLDP, используемого для обнаружения соседних сетевых устройств на канальном уровне.

Также поддерживается режим совместимости с протоколом CDP. Если Numa Edge получит сообщение протокола CDP, то он перестанет передавать LLDP на указанном порту, и будет передавать CDP сообщения.

Форма **set** данной команды используется для указания режима работы протокола LLDP.

Форма **delete** данной команды используется установление режима работы протокола LLDP в значение по умолчанию.

Форма **show** данной команды используется для отображения режима работы протокола LLDP.

10.2.2 interfaces ethernet <ethx> mac <mac-адрес>

Назначение MAC-адреса для интерфейса Ethernet.

Синтаксис

```
set interfaces ethernet <ethx> mac <mac-адрес>

delete interfaces ethernet <ethx> mac

show interfaces ethernet <ethx> mac
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      mac mac-адрес
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

mac-адрес

MAC-адрес, который будет назначен интерфейсу Ethernet. Адрес указывается в формате шести разделенных двоеточиями 8-битовых шестнадцатеричных чисел, например, 00:0a:59:9a:f2:ba.

Значение по умолчанию

По умолчанию установлен MAC-адрес, присвоенный производителем.

Указания по использованию

Команда используется для установки MAC-адреса интерфейса Ethernet. Это значение заменит MAC-адрес, установленный при изготовлении сетевой платы.

Форма **set** данной команды используется для назначения MAC-адреса интерфейсу.

Форма **delete** данной команды используется для восстановления MAC-адреса, присвоенного производителем сетевой карты.

Форма **show** данной команды используется для отображения настройки MAC-адреса.

10.2.3 interfaces ethernet <ethx> mtu <mtu>

Установка значения MTU для интерфейса Ethernet.

Синтаксис

```
set interfaces ethernet <ethx> mtu <mtu>
delete interfaces ethernet <ethx> mtu
show interfaces ethernet <ethx> mtu
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    ethernet ethx {
        mtu mtu
    }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

mtu

Установка значения MTU для интерфейса Ethernet. Значение должно лежать в диапазоне от 68 до 9000.

Значение по умолчанию

По умолчанию значение MTU устанавливается равным 1500.

Указания по использованию

Команда позволяет установить значение MTU (максимальный размер передаваемого блока данных) для интерфейса Ethernet. Если на редактируемом интерфейсе также настроены логические интерфейсы, то устанавливаемое значение MTU должно быть не меньше, чем на логическом интерфейсе.

При перенаправлении пакеты IPv4, имеющие размер больший, чем значение MTU, будут фрагментированы, за исключением случая, когда установлен флаг DF. В этом случае пакеты будут проигнорированы.

Форма **set** данной команды используется для установки значения MTU.

Форма **delete** данной команды используется для удаления установленного значения MTU и отключения фрагментации.

Форма **show** данной команды используется для отображения настройки MTU.

10.2.4 interfaces ethernet <ethx> speed <скорость>

Установка скорости интерфейса Ethernet.

Синтаксис

```
set interfaces ethernet <ethx> speed <скорость>
delete interfaces ethernet <ethx> speed
show interfaces ethernet <ethx> speed
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      speed скорость
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

скорость

Устанавливаемая скорость интерфейса Ethernet. Допустимые значения представлены в таблице ниже.

Таблица 36 – Скорости интерфейса Ethernet

Значение	Описание
auto	Скорость интерфейса будет автоматически согласована маршрутизатором с интерфейсом на другом конце подключения.
10	10 Мбит/с
100	100 Мбит/с
1000	1 Гбит/с
2500	2,5Гбит/с
10000	10 Гбит/с

Значение по умолчанию

Значение скорости для канала Ethernet устанавливается автоматически.

Указания по использованию

Команда используется для установки скорости интерфейса Ethernet. Если режим дуплекса устанавливается явно, то также потребуется явно указать значение параметра **interfaces ethernet ethx duplex**.

ПРИМЕЧАНИЕ Оборудование может не поддерживать возможность явной установки скорости передачи (или определенные режимы работы). Если используется оборудование, не поддерживающее такую установку (или определенные режимы работы), при фиксации изменений будет отображено сообщение об ошибке.

Форма **set** данной команды используется для установки скорости интерфейса.

Форма **delete** данной команды используется для восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки скорости.

10.2.5 clear interfaces ethernet <ethx> counters

Очистка статистических счетчиков для интерфейса Ethernet.

Синтаксис

```
clear interfaces ethernet <ethx>  counters
```

Режим интерфейса

Эксплуатационный режим.

Параметры

ethx

Идентификатор интерфейса Ethernet, для которого требуется очистить статистические счетчики. Значение должно лежать в диапазоне от eth0 до eth999 в зависимости от реально имеющихся в системе интерфейсов Ethernet.

Значение по умолчанию

Очистка счетчиков для всех интерфейсов Ethernet.

Указания по использованию

Команда позволяет очистить счетчики для интерфейсов Ethernet. Просмотреть значения счетчиков можно при помощи команды **show interfaces counters**.

10.2.6 show interfaces ethernet

Вывод сведений и статистических данных для интерфейсов Ethernet.

Синтаксис

```
show interfaces ethernet [detail | <ethx> [brief | capture [not port <порт> | port <порт>] | identify | physical | queue [class | filter] | statistics]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

detail

Отображение подробных сведений об интерфейсах Ethernet.

ethx

Отображение сведений для указанного интерфейса Ethernet.

brief

Отображение кратких сведений о состоянии для указанного интерфейса Ethernet.

capture

Перехват и отображение трафика на указанном интерфейсе Ethernet.

not port *порт*

Отображение сетевого трафика, записанного на всех портах, кроме указанного.

port *порт*

Отображение сетевого трафика, записанного на указанном порту.

identity

Включение светодиодного индикатора на интерфейсе Ethernet для его определения.

physical

Отображение сведений о физическом уровне для указанного интерфейса Ethernet.

queue

Отображение сведений об очередях для интерфейса Ethernet.

class

Отображение классов очередей для указанного интерфейса.

filter

Отображение фильтров очередей для указанного интерфейса.

statistics

Отображение аппаратной статистики для адаптеров Ethernet.

Значение по умолчанию

Отображение сведений для всех интерфейсов Ethernet.

Указания по использованию

Команда используется для просмотра состояния интерфейса Ethernet.

Примеры

В примере ниже выводятся сведения для всех интерфейсов Ethernet.

Пример 93– Вывод сведений для всех интерфейсов Ethernet

```
admin@edge:~$ show interfaces ethernet
Interface    IP Address          State       Link   Description
eth1         -                   admin down  down
eth2         192.168.10.1/24     up          up
eth3         192.168.11.254/24   up          up
admin@edge:~$
```

В примере ниже выводятся сведения для интерфейса eth2.

Пример 94– Вывод сведений для одного интерфейса Ethernet

```
admin@edge:~$ show interfaces ethernet eth2
eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:a9:35:13 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.1/24 brd 192.168.10.255 scope global eth2
       valid_lft forever preferred_lft forever

    RX:  bytes    packets     errors    dropped    overrun      mcast
        127085       1461          0          3          0          0
    TX:  bytes    packets     errors    dropped    carrier collisions
         85248        752          0          0          0          0

admin@edge:~$
```

10.3 Настройка интерфейса заглушки

В данном разделе представлены следующие команды.

Команды настройки	
interfaces loopback lo	Определение интерфейса заглушки.
interfaces loopback lo address <ip-адрес>	Назначение интерфейсу заглушки IP-адреса и префикса сети.
interfaces loopback lo description <описание>	Текстовое описание интерфейса заглушки.
Эксплуатационные команды	
clear interfaces loopback counters	Очистка статистических счетчиков для интерфейса заглушки.
show interfaces loopback	Отображение сведений об интерфейсе заглушки.

10.3.1 interfaces loopback lo

Определение интерфейса заглушки.

Синтаксис

```
set interfaces loopback lo

delete interfaces loopback lo

show interfaces loopback
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   loopback lo
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для определения интерфейса заглушки.

Интерфейс заглушки представляет собой специализированный программный интерфейс, эмулирующий физический интерфейс, который служит для организации подключения системы к самой себе. Пакеты, маршрутизированные на интерфейс loopback, маршрутизируются назад в систему и обрабатываются локально. Пакеты, маршрутизированные на интерфейс заглушки и при этом предназначенные не для интерфейса заглушки, отбрасываются.

Форма **set** данной команды используется для создания конфигурации интерфейса заглушки.

Форма **delete** данной команды используется для удаления конфигурации интерфейса заглушки. При следующем запуске системы для интерфейса будет создан пустой узел конфигурации.

Форма **show** данной команды используется для отображения настройки интерфейса Ethernet.

10.3.2 interfaces loopback lo address <ip-адрес>

Назначение интерфейсу заглушки IP-адреса и префикса сети.

Синтаксис

```
set interfaces loopback lo address <ip-адрес>
delete interfaces loopback lo address [<ip-адрес>]
show interfaces loopback lo address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   loopback lo {
      address ip-адрес
   }
}
```

Параметры

ip-адрес

IPv4-адрес или IPv6-адрес для интерфейса заглушки. Допустимые значения представлены в таблице ниже:

Таблица 37 – Формат указания ip-адреса для интерфейса

Значение	Описание
<x.x.x.x/x>	IPv4-адрес/префикс (например: 192.168.10.254/24).
<h:h:h:h:h:h:h:h/x>	IPv6-адрес/префикс (например, 2001:db8:1234::/48)

Назначить интерфейсу несколько IP-адресов можно, создав соответствующее количество узлов конфигурации **address.**

Значение по умолчанию

Отсутствует.

Указания по использованию

IP-адрес интерфейса заглушки должен быть уникальным и не должен использоваться другими интерфейсами.

При настройке системы может быть полезно воспользоваться надежностью интерфейса заглушки:

- Имя узла системы рекомендуется сопоставить с адресом интерфейса заглушки, а не физического интерфейса;
- При настройке OSPF и iBGP в качестве идентификатора маршрутизатора рекомендуется установить адрес интерфейса заглушки.

Форма **set** данной команды используется для назначения IP-адреса и префикса сети. Чтобы назначить интерфейсу несколько IP-адресов, следует создать соответствующее количество узлов конфигурации **address**.

Форма **delete** данной команды используется для удаления адреса интерфейса заглушки.

Форма **show** данной команды используется для отображения настройки интерфейса заглушки.

10.3.3 interfaces loopback lo description <описание>

Текстовое описание интерфейса заглушки.

Синтаксис

```
set interfaces loopback lo description <описание>
delete interfaces loopback lo description
show interfaces loopback lo description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   loopback lo {
      description описание
   }
}
```

Параметры

описание

Мнемоническое имя или описание интерфейса заглушки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда позволяет установить текстовое описание интерфейса заглушки.

Форма **set** данной команды используется для установки описания.

Форма **delete** данной команды используется для удаления описания.

Форма **show** данной команды используется для отображения настройки описания.

10.3.4 clear interfaces loopback counters

Очистка статистических счетчиков для интерфейса заглушки.

Синтаксис

```
clear interfaces loopback [lo] counters
```

Режим интерфейса

Эксплуатационный режим.

Параметры

lo

Необязательный параметр. Очистка статистики только для интерфейса **lo**.

Значение по умолчанию

Очистка счетчиков для всех интерфейсов заглушки.

Указания по использованию

Команда используется для очистки счетчиков на интерфейсах заглушки. Просмотреть значения счетчиков можно при помощи команды **show interfaces counters**.

10.3.5 show interfaces loopback

Вывод сведений об интерфейсе заглушки.

Синтаксис

```
show interfaces loopback [detail | lo [brief | capture [not port <порт> |
port <порт>] | queue [class | filter]]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

detail

Вывод подробных сведений и статистических данных для интерфейса заглушки.

lo

Отображение подробных сведений о настройке и статистических данных для интерфейса заглушки.

brief

Отображение кратких сведений о состоянии для указанного интерфейса заглушки.

capture

Перехват и отображение трафика на интерфейсе заглушке.

not port *порт*

Отображение сетевого трафика, записанного на всех портах, кроме указанного.

port *порт*

Отображение сетевого трафика, записанного на указанном порту.

queue

Отображение сведений об очередях для интерфейса заглушки.

class

Отображение классов очередей для указанного интерфейса.

filter

Отображение фильтров очередей для указанного интерфейса.

Значение по умолчанию

Вывод кратких сведений о состоянии интерфейса заглушки.

Указания по использованию

Команда используется для отображения состояния интерфейса заглушки.

Примеры

В примере ниже приведен вывод сведений для интерфейса заглушки.

Пример 95– Вывод сведений об интерфейсе заглушки

```
admin@edge:~$ show interfaces loopback
Interface    IP Address         State       Link   Description
lo           127.0.0.1/8        up          up
lo           ::1/128            up          up
```

В примере ниже приведен вывод подробных сведений для интерфейса заглушки.

Пример 96– Вывод подробных сведений для интерфейса заглушки

```
admin@edge:~$ show interfaces loopback detail
lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever

    RX:  bytes    packets     errors    dropped    overrun      mcast
          1158         16          0          0          0          0
    TX:  bytes    packets     errors    dropped    carrier collisions
          1158         16          0          0          0          0
```

10.4 Настройка виртуальных интерфейсов

В данном разделе представлены следующие команды.

Команды настройки	
Виртуальные интерфейсы на интерфейсах Ethernet	
interfaces ethernet <ethx> vif <идентификатор_vlan>	Определение виртуального интерфейса на интерфейсе Ethernet.
interfaces ethernet <ethx> vif <идентификатор_vlan> address	Назначение IP-адреса и префикса сети для виртуального интерфейса Ethernet.
interfaces ethernet <ethx> vif <идентификатор_vlan> description <описание>	Текстовое описание виртуального интерфейса на интерфейсе Ethernet.
interfaces ethernet <ethx> vif <идентификатор_vlan> disable	Отключение виртуального интерфейса с сохранением текущей настройки.
interfaces ethernet <ethx> vif <идентификатор_vlan> enable-proxy-arp	Включение режима проксирования ARP для виртуального интерфейса Ethernet.
interfaces ethernet <ethx> vif <идентификатор_vlan> mtu <mtu>	Установка значения MTU для виртуального интерфейса на интерфейсе Ethernet.
Виртуальные интерфейсы на интерфейсах агрегированных каналов Ethernet	
interfaces bonding <bondx> vif <идентификатор_vlan>	Определение виртуального интерфейса на интерфейсе агрегированных каналов Ethernet.
interfaces bonding <bondx> vif <идентификатор_vlan> address	Назначение IP-адреса и префикса сети для виртуального интерфейса агрегированных каналов Ethernet.
interfaces bonding <bondx> vif <идентификатор_vlan> description <описание>	Текстовое описание виртуального интерфейса агрегированных каналов Ethernet.
interfaces bonding <bondx> vif <идентификатор_vlan> disable	Отключение виртуального интерфейса с сохранением текущей настройки.

interfaces bonding <bondx> vif <идентификатор_vlan> enable-proxy-arp	Включение режима проксирования ARP для виртуальных агрегированных интерфейсов Ethernet.
interfaces bonding <bondx> vif <идентификатор_vlan> mtu <mtu>	Установка значения MTU для виртуальных агрегированных интерфейсов Ethernet.
Эксплуатационные команды	
show interfaces ethernet <ethx> vif <идентификатор_vlan>	Отображение сведений о виртуальном интерфейсе Ethernet.
show interfaces bonding <bondx> vif <идентификатор_vlan>	Отображение сведений о виртуальном интерфейсе агрегированных каналов Ethernet.

10.4.1 interfaces ethernet <ethx> vif <идентификатор_vlan>

Определение виртуального интерфейса на интерфейсе Ethernet.

Синтаксис

```
set interfaces ethernet <ethx> vif <идентификатор_vlan>
delete interfaces ethernet <ethx> vif <идентификатор_vlan>
show interfaces ethernet <ethx> vif <идентификатор_vlan>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      vif идентификатор_vlan {
      }
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

идентификатор_vlan

Множественный узел. Идентификатор VLAN для виртуального интерфейса, используемый с системой тегов VLAN стандарта 802.1Q. Значение должно лежать в диапазоне от 1 до 4094. Следует отметить, что на виртуальном интерфейсе Ethernet будут обрабатываться только сетевые пакеты, имеющие теги стандарта 802.1Q. Для одного интерфейса Ethernet можно определить несколько виртуальных интерфейсов, для этого следует создать соответствующее количество узлов конфигурации **vif.**

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для создания виртуального интерфейса Ethernet.

Виртуальные интерфейсы Ethernet обрабатывают только сетевой трафик, имеющий теги стандарта 802.1Q.

Форма **set** данной команды используется для создания виртуального интерфейса.

Форма **delete** данной команды используется для удаления виртуального интерфейса, а также всех его настроек.

Форма **show** данной команды используется для отображения настройки виртуального интерфейса Ethernet.

10.4.2 interfaces ethernet <ethx> vif <идентификатор_vlan> address

Назначение IP-адреса и префикса сети для виртуального интерфейса Ethernet.

Синтаксис

```
set interfaces ethernet <ethx> vif <идентификатор_vlan> address [<ip-адрес> | dhcp]

delete interfaces ethernet <ethx> vif <идентификатор_vlan> address [<ip-адрес> | dhcp]

show interfaces ethernet <ethx> vif <идентификатор_vlan>address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      vif идентификатор_vlan {
         address ip-адрес | dhcp
      }
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

идентификатор_vlan

Множественный узел. Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 1 до 4094.

ip-адрес

IPv4-адрес или IPv6-адрес для данного виртуального интерфейса Ethernet. Допустимые значения представлены в таблице ниже:

Таблица 38 – Формат указания ip-адреса для интерфейса

Значение	Описание
<x.x.x.x/x>	IPv4-адрес/префикс (например: 192.168.10.254/24).
<h:h:h:h:h:h:h:h/x>	IPv6-адрес/префикс (например, 2001:db8:1234::/48)

Назначить интерфейсу несколько IP-адресов можно, создав соответствующее количество узлов конфигурации **address.**

dhcp

Параметр определяет интерфейса как клиент протокола DHCP, получающий адрес и префикс от сервера DHCP.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды позволяет назначить IP-адрес указанному виртуальному интерфейсу.

Форма **delete** данной команды используется для удаления IP-адреса для указанного виртуального интерфейса.

Форма **show** данной команды используется для отображения настройки IP-адреса указанного виртуального интерфейса.

10.4.3 interfaces ethernet <ethx> vif <идентификатор_vlan> description <описание>

Текстовое описание виртуального интерфейса на интерфейсе Ethernet.

Синтаксис

```
set interfaces ethernet <ethx> vif <идентификатор_vlan> description <описание>

delete interfaces ethernet <ethx> vif <идентификатор_vlan> description

show interfaces ethernet <ethx> vif <идентификатор_vlan> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    ethernet ethx {
        vif идентификатор_vlan {
            description описание
        }
    }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

идентификатор_vlan

Множественный узел. Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 1 до 4094.

описание

Мнемоническое имя или описание интерфейса Ethernet.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для создания текстового описания для виртуального интерфейса Ethernet.

Форма **set** данной команды используется для создания текстового описания.

Форма **delete** данной команды используется для удаления текстового описания виртуального интерфейса.

Форма **show** данной команды используется для отображения настройки текстового описания виртуального интерфейса.

10.4.4 interfaces ethernet <ethx> vif <идентификатор_vlan> disable

Отключение виртуального интерфейса Ethernet с сохранением текущей настройки.

Синтаксис

```
set interfaces ethernet <ethx> vif <идентификатор_vlan> disable

delete interfaces ethernet <ethx> vif <идентификатор_vlan> disable

show interfaces ethernet <ethx> vif <идентификатор_vlan>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    ethernet ethx {
```

```
        vif идентификатор_vlan {
            disable
        }
    }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

идентификатор_vlan

Множественный узел. Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 1 до 4094.

Значение по умолчанию

Виртуальный интерфейс включен.

Указания по использованию

Команда позволяет отключить виртуальный интерфейс Ethernet без удаления настройки.

Форма **set** данной команды используется для отключения интерфейса.

Форма **delete** данной команды используется для включения интерфейса.

Форма **show** данной команды используется для отображения настройки виртуального интерфейса Ethernet.

10.4.5 interfaces ethernet <ethx> vif <идентификатор_vlan> enable-proxy-arp

Включение режима проксирования ARP для виртуального интерфейса Ethernet.

Синтаксис

```
set interfaces ethernet <ethx> vif <идентификатор_vlan> enable-proxy-arp
delete interfaces ethernet <ethx> vif <идентификатор_vlan> enable-proxy-arp
show interfaces ethernet <ethx> vif <идентификатор_vlan>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    ethernet ethx {
        vif идентификатор_vlan {
            enable-proxy-arp
        }
    }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого виртуального интерфейса Ethernet.

идентификатор_vlan

Множественный узел. Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 1 до 4094.

Значение по умолчанию

Режим проксирования ARP для виртуального интерфейса Ethernet отключен.

Указания по использованию

Команда используется для включения режима проксирования ARP (Address Resolution Protocol) для виртуального интерфейса Ethernet.

Режим проксирования ARP позволяет виртуальному интерфейсу Ethernet отвечать на запросы ARP (используя свой собственный MAC-адрес) в том случае, если IP-адрес назначения принадлежит подсетям, подключенным к другим интерфейсам системы. Последующие пакеты для данного IP-адреса назначения будут соответствующим образом перенаправляться системой.

Форма **set** данной команды используется для включения режима проксирования ARP для виртуального интерфейса Ethernet.

Форма **delete** данной команды используется для восстановления поведения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки.

10.4.6 interfaces ethernet <ethx> vif <идентификатор_vlan> mtu <mtu>

Установка значения MTU для виртуального интерфейса Ethernet.

Синтаксис

```
set interfaces ethernet <ethx> vif <идентификатор_vlan> mtu <mtu>
delete interfaces ethernet <ethx> vif <идентификатор_vlan> mtu
show interfaces ethernet <ethx> vif <идентификатор_vlan> mtu
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    ethernet ethx {
        vif идентификатор_vlan {
            mtu mtu
        }
    }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

идентификатор_vlan

Множественный узел. Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 1 до 4094.

mtu

Установка значения MTU для виртуального интерфейса Ethernet. Значение должно лежать в диапазоне от 68 до 9000.

Значение по умолчанию

По умолчанию значение MTU устанавливается равным 1500.

Указания по использованию

Команда позволяет установить значение MTU (максимальный размер передаваемого блока данных) для виртуального интерфейса Ethernet.

ПРИМЕЧАНИЕ Значение MTU, устанавливаемое для виртуального интерфейса Ethernet не может превышать значения MTU родительского интерфейса.

При перенаправлении пакеты IPv4, имеющие размер больший, чем значение MTU, будут фрагментированы, за исключением случая, когда установлен флаг DF. В этом случае пакеты будут проигнорированы.

Форма **set** данной команды используется для установки значения MTU.

Форма **delete** данной команды используется для удаления установленного значения MTU и отключения фрагментации.

Форма **show** данной команды используется для отображения настройки MTU.

10.4.7 interfaces bonding <bondx> vif <идентификатор_vlan>

Определение виртуального интерфейса на интерфейсе агрегированных каналов Ethernet.

Синтаксис

```
set interfaces bonding <bondx> vif <идентификатор_vlan>
delete interfaces bonding <bondx> vif <идентификатор_vlan>
show interfaces bonding <bondx> vif <идентификатор_vlan>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bonding bondx {
      vif идентификатор_vlan {
      }
   }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от bond0 до bond99.

идентификатор_vlan

Множественный узел. Идентификатор VLAN для виртуального интерфейса, используемый с системой тегов VLAN стандарта 802.1Q. Значение должно лежать в диапазоне от 1 до 4094. Следует отметить, что на виртуальном интерфейсе агрегированных каналов Ethernet будут обрабатываться только сетевые пакеты, имеющие теги стандарта 802.1Q. Для одного интерфейса агрегированных каналов Ethernet можно определить несколько виртуальных интерфейсов, для этого следует создать соответствующее количество узлов конфигурации **vif**.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для создания виртуального интерфейса агрегированных каналов Ethernet.

Форма **set** данной команды используется для создания виртуального интерфейса.

Форма **delete** данной команды используется для удаления виртуального интерфейса и всей его настройки.

Форма **show** данной команды используется для просмотра настройки виртуального интерфейса.

10.4.8 interfaces bonding <bondx> vif <идентификатор_vlan> address

Назначение IP-адреса и префикса сети для виртуального интерфейса агрегированных каналов Ethernet.

Синтаксис

```
set interfaces bonding <bondx> vif <идентификатор_vlan> address [<ip-адрес> |
dhcp]
```

```
delete interfaces bonding <bondx> vif <идентификатор_vlan> address [<ip-адрес> | dhcp]
show interfaces bonding <bondx> vif <идентификатор_vlan> address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bonding bondx {
       vif идентификатор_vlan {
          address ip-адрес | dhcp
       }
   }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от bond0 до bond99.

идентификатор_vlan

Множественный узел. Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 1 до 4094.

ip-адрес

IPv4-адрес или IPv6-адрес для данного виртуального интерфейса агрегированных каналов Ethernet. Допустимые значения представлены в таблице ниже:

Таблица 39 – Формат указания ip-адреса для интерфейса

Значение	Описание
<x.x.x.x/x>	IPv4-адрес/префикс (например: 192.168.10.254/24).
<h:h:h:h:h:h:h:h/x>	IPv6-адрес/префикс (например, 2001:db8:1234::/48)

Назначить интерфейсу несколько IP-адресов можно, создав соответствующее количество узлов конфигурации **address.**

dhcp

Параметр определяет интерфейс как клиент протокола DHCP, получающий адрес и префикс от сервера DHCP.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды позволяет назначить IP-адрес указанному виртуальному интерфейсу.

Форма **delete** данной команды позволяет удалить IP-адрес для указанного виртуального интерфейса.

Форма **show** данной команды используется для отображения настройки IP-адреса указанного виртуального интерфейса.

10.4.9 interfaces bonding <bondx> vif <идентификатор_vlan> description <описание>

Текстовое описание виртуального интерфейса агрегированных каналов Ethernet.

Синтаксис

```
set interfaces bonding <bondx> vif <идентификатор_vlan> description <описание>
```

```
delete interfaces bonding <bondx> vif <идентификатор_vlan> description
show interfaces bonding <bondx> vif <идентификатор_vlan> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bonding bondx {
      vif идентификатор_vlan {
         description описание
      }
   }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от bond0 до bond99.

идентификатор_vlan

Множественный узел. Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 1 до 4094.

описание

Мнемоническое имя или описание виртуального интерфейса.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для создания текстового описания для виртуального интерфейса агрегированных каналов Ethernet.

Форма **set** данной команды используется для создания текстового описания виртуального интерфейса.

Форма **delete** данной команды используется для удаления текстового описания виртуального интерфейса.

Форма **show** данной команды используется для отображения текстового описания виртуального интерфейса.

10.4.10 interfaces bonding <bondx> vif <идентификатор_vlan> disable

Отключение виртуального интерфейса агрегированных каналов Ethernet с сохранением текущей настройки.

Синтаксис

```
set interfaces bonding <bondx> vif <идентификатор_vlan> disable
delete interfaces bonding <bondx> vif <идентификатор_vlan> disable
show interfaces bonding <bondx> vif <идентификатор_vlan>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bonding bondx {
      vif идентификатор_vlan {
```

```
            disable
        }
    }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от bond0 до bond99.

идентификатор_vlan

Множественный узел. Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 1 до 4094.

Значение по умолчанию

Виртуальный интерфейс включен.

Указания по использованию

Команда используется для отключения виртуального интерфейса агрегированных каналов Ethernet с сохранением настроек.

Форма **set** данной команды используется для отключения интерфейса.

Форма **delete** данной команды используется для включения интерфейса.

Форма **show** данной команды используется для просмотра настройки.

10.4.11 interfaces bonding <bondx> vif <идентификатор_vlan> enable-proxy-arp

Включение режима проксирования ARP для виртуальных агрегированных интерфейсов Ethernet.

Синтаксис

```
set interfaces bonding <bondx> vif <идентификатор_vlan> enable-proxy-arp
delete interfaces bonding <bondx> vif <идентификатор_vlan> enable-proxy-arp
show interfaces bonding <bondx> vif <идентификатор_vlan>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    bonding bondx {
        vif идентификатор_vlan {
            enable-proxy-arp
        }
    }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от bond0 до bond99.

идентификатор_vlan

Множественный узел. Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 1 до 4094.

Значение по умолчанию

Режим проксирования ARP для виртуальных агрегированных интерфейсов Ethernet отключен.

Указания по использованию

Команда используется для включения режима проксирования ARP (Address Resolution Protocol) для виртуального агрегированного интерфейса Ethernet.

Форма **set** данной команды используется для включения режима проксирования ARP для виртуального агрегированного интерфейса Ethernet.

Форма **delete** данной команды используется для восстановления поведения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки.

10.4.12 interfaces bonding <bondx> vif <идентификатор_vlan> mtu <mtu>

Установка значения MTU для виртуального интерфейса агрегированных каналов Ethernet.

Синтаксис

```
set interfaces bonding <bondx> vif <идентификатор_vlan> mtu <mtu>
delete interfaces bonding <bondx> vif <идентификатор_vlan> mtu
show interfaces bonding <bondx> vif <идентификатор_vlan> mtu
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bonding bondx {
      vif идентификатор_vlan {
         mtu mtu
      }
   }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от bond0 до bond99.

идентификатор_vlan

Множественный узел. Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 1 до 4094.

mtu

Установка значения MTU для виртуального интерфейса агрегированных каналов Ethernet. Значение должно лежать в диапазоне от 68 до 9000.

Значение по умолчанию

По умолчанию значение MTU устанавливается равным 1500.

Указания по использованию

Команда позволяет установить значение MTU (максимальный размер передаваемого блока данных) для виртуального интерфейса агрегированных каналов Ethernet.

ПРИМЕЧАНИЕ Значение MTU, устанавливаемое для виртуального интерфейса агрегированных каналов Ethernet не может превышать значения MTU родительского интерфейса.

При перенаправлении пакеты IPv4, имеющие размер больший, чем значение MTU, будут фрагментированы, за исключением случая, когда установлен флаг DF. В этом случае пакеты будут проигнорированы.

Форма **set** данной команды используется для установки значения MTU.

Форма **delete** данной команды используется для удаления установленного значения MTU и отключения фрагментации.

Форма **show** данной команды используется для отображения настройки MTU.

10.4.13 show interfaces ethernet <ethx> vif <идентификатор_vlan>

Вывод сведений о виртуальном интерфейсе Ethernet.

Синтаксис

```
show interfaces ethernet <ethx> vif <идентификатор_vlan> [brief | capture [not port <порт> | port <порт>] | queue [class | filter]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

ethx

Идентификатор определяемого интерфейса Ethernet.

идентификатор_vlan

Отображение сведений для указанного виртуального интерфейса.

brief

Отображение кратких сведений о состоянии для указанного виртуального интерфейса Ethernet.

capture

Перехват и отображение трафика на указанном виртуальном интерфейсе Ethernet.

not port *порт*

Отображение сетевого трафика, записанного на всех портах, кроме указанного.

port *порт*

Отображение сетевого трафика, записанного на указанном порту.

queue

Отображение сведений об очередях для виртуального интерфейса Ethernet.

class

Отображение классов очередей для указанного интерфейса.

filter

Отображение фильтров очередей для указанного интерфейса.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для отображения состояния управления и работоспособности виртуального интерфейса Ethernet.

Примеры

В примере ниже приведен вывод сведений для виртуального интерфейса vif 10, настроенного на интерфейсе eth1.

Пример 97- Вывод сведений для виртуального интерфейса Ethernet

```
admin@edge:~$ show interfaces ethernet eth1 vif 10
eth1.10@eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state
UP group default qlen 1000
    link/ether 0c:8a:a5:22:e9:01 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.254/24 brd 192.168.3.255 scope global eth1.10
       valid_lft forever preferred_lft forever
    inet6 fe80::e8a:a5ff:fe22:e901/64 scope link
       valid_lft forever preferred_lft forever

    RX:  bytes    packets     errors    dropped    overrun      mcast
              0          0          0          0          0          0
    TX:  bytes    packets     errors    dropped    carrier collisions
            896          8          0          0          0          0
```

В примере ниже приведен вывод кратких сведений для виртуального интерфейса vif 10, настроенного на интерфейсе eth1.

Пример 98- Вывод кратких сведений сведений для виртуального интерфейса Ethernet

```
admin@edge02:~$ show interfaces ethernet eth1 vif 10 brief
Interface    IP Address         State       Link   Description
eth1.10      192.168.1.254/24   up          up
```

10.4.14 show interfaces bonding <bondx> vif <идентификатор_vlan>

Вывод сведений о виртуальном интерфейсе агрегированных каналов Ethernet.

Синтаксис

```
show interfaces bonding <bondx> vif <идентификатор_vlan> [brief | capture
[not port <порт> | port <порт>] | queue [class | filter]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

bondx

Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от bond0 до bond99.

идентификатор_vlan

Отображение сведений для указанного виртуального интерфейса.

brief

Отображение сведений о состоянии для виртуального интерфейса агрегированных каналов Ethernet.

capture

Перехват и отображение трафика на указанном виртуальном интерфейсе агрегированных каналов Ethernet.

not port *порт*

Отображение сетевого трафика, записанного на всех портах, кроме указанного.

port *порт*

Отображение сетевого трафика, записанного на указанном порту.

queue

Отображение сведений об очередях для виртуального интерфейса агрегированных каналов Ethernet.

class

Отображение классов очередей для указанного интерфейса.

filter

Отображение фильтров очередей для указанного интерфейса.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда позволяет просмотреть состояние управления и работоспособности виртуального интерфейса агрегированных каналов Ethernet.

Примеры

В примере ниже приведен вывод сведений для виртуального интерфейса vif 10, созданного на основе интерфейса агрегированных каналов bond0.

Пример 99– Вывод сведений для виртуального интерфейса агрегированных каналов

```
admin@edge:~$ show  interfaces bonding bond0 vif 10
bond0.10@bond0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state
UP group default qlen 1000
    link/ether 08:00:27:19:99:28 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::a00:27ff:fe19:9928/64 scope link
       valid_lft forever preferred_lft forever

    RX:  bytes    packets     errors    dropped    overrun      mcast
               0          0          0          0          0          0
    TX:  bytes    packets     errors    dropped    carrier collisions
             746          7          0          0          0          0
```

В примере ниже приведен вывод кратких сведений для виртуального интерфейса vif 10, созданного на основе интерфейса агрегированных каналов bond0.

Пример 100– Вывод кратких сведений для виртуального интерфейса агрегированных каналов

```
admin@edge:~$ show  interfaces bonding bond0 vif 10 brief
Interface    IP Address         State       Link   Description
bond0.10     -                  up          up
```

10.5 Настройка мостов

В данном разделе представлены следующие команды.

Команды настройки	
Мостовые группы	
interfaces bridge <brx>	Определение мостовой группы.
interfaces bridge <brx> address	Назначение адреса мостовой группе.
interfaces bridge <brx> aging <время_хранения>	Установка интервала времени, в течение которого MAC-адрес хранится в таблице пересылки мостовой группы.
interfaces bridge <brx> description <описание>	Текстовое описание мостовой группы.
interfaces bridge <brx> disable	Отключение мостовой группы с сохранением настройки.
interfaces bridge <brx> enable-proxy-arp	Включение режима проксирования ARP для мостового интерфейса Ethernet.
interfaces bridge <brx> forwarding-delay <время_задержки>	Установка времени задержки пересылки, в течение которого мостовая группа продолжает прослушивание после изменения топологии.
interfaces bridge <brx> hello-time <интервал>	Интервал времени, через который мостовая группа отправляет пакет "hello".
interfaces bridge <brx> max-age <интервал>	Установка времени ожидания мостовой группой пакета

	"hello" от корня связующего дерева.
interfaces bridge <brx> priority <приоритет>	Установка приоритета пересылки для мостовой группы в связующем дереве.
interfaces bridge <brx> stp <состояние>	Включение протокола STP (IEEE 802.1D Spanning Tree Protocol) для мостовой группы.
Интерфейсы Ethernet	
interfaces ethernet <ethx> bridge-group bridge <brx>	Включение интерфейса Ethernet в состав мостовой группы.
interfaces ethernet <ethx> bridge-group cost <стоимость>	Установка стоимости пути для интерфейса Ethernet, входящего в состав мостовой группы.
interfaces ethernet <ethx> bridge-group priority <приоритет>	Установка приоритета для интерфейса Ethernet, входящего в состав мостовой группы.
Виртуальные интерфейсы Ethernet	
interfaces ethernet <ethx> vif <идентификатор_vlan> bridge-group bridge <brx>	Включение виртуального интерфейса в состав мостовой группы.
interfaces ethernet <ethx> vif <идентификатор_vlan> bridge-group cost <стоимость>	Установка стоимости пути для виртуального интерфейса Ethernet, входящего в состав мостовой группы.
interfaces ethernet <ethx> vif <идентификатор_vlan> bridge-group priority <приоритет>	Установка приоритета для виртуального интерфейса Ethernet, входящего в состав мостовой группы.
Туннельные интерфейсы	
interfaces tunnel <tunx> bridge-group bridge <brx>	Включение туннельного интерфейса GRE в состав мостовой группы.
interfaces tunnel <tunx> bridge-group cost <стоимость>	Установка стоимости пути для туннельного интерфейса GRE, входящего в состав мостовой группы.
interfaces tunnel <tunx> bridge-group priority <приоритет>	Установка приоритета для туннельного интерфейса GRE, входящего в состав мостовой группы.
Интерфейсы агрегированных каналов Ethernet	
interfaces bonding <bondx> bridge-group bridge <brx>	Включение интерфейса агрегированных каналов Ethernet в состав мостовой группы.
interfaces bonding <bondx> bridge-group cost <стоимость>	Установка стоимости пути для интерфейса агрегированных каналов Ethernet, входящего в состав мостовой группы.
interfaces bonding <bondx> bridge-group priority <приоритет>	Установка приоритета для интерфейса агрегированных каналов Ethernet, входящего в состав мостовой группы.
Виртуальные интерфейсы агрегированных каналов Ethernet	
interfaces bonding <bondx> vif <идентификатор_vlan> bridge-group bridge <brx>	Включение виртуального интерфейса агрегированных каналов Ethernet в состав мостовой группы.
interfaces bonding <bondx> vif <идентификатор_vlan> bridge-group cost <стоимость>	Установка стоимости пути для виртуального интерфейса агрегированных каналов Ethernet, входящего в состав мостовой группы.
interfaces bonding <bondx> vif <идентификатор_vlan> bridge-group priority <приоритет>	Установка приоритета для виртуального интерфейса агрегированных каналов Ethernet, входящего в состав мостовой группы.
Эксплуатационные команды	
clear interfaces bridge counters	Очистка статистической информации для интерфейса моста.
show bridge	Вывод сведений об активных мостовых группах.
show interfaces bridge	Вывод сведений об интерфейсе сетевого моста.

10.5.1 interfaces bridge <brx>

Определение мостовой группы.

Синтаксис

```
set interfaces bridge <brx>
delete interfaces bridge <brx>
show interfaces bridge <brx>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bridge brx {
   }
}
```

Параметры

brx

Множественный узел. Идентификатор мостовой группы. Значение должно лежать в диапазоне от br0 до br999. Для того чтобы определить несколько мостовых групп, следует создать соответствующее количество узлов конфигурации **bridge.**

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для определения мостовой группы. Обратите внимание, что включить интерфейс в мостовую группу можно только после того, как он будет определен.

Форма **set** данной команды используется для создания мостовой группы и указания ее настроек.

Форма **delete** данной команды используется для удаления всех настроек для мостовой группы.

Форма **show** данной команды используется для отображения настройки мостовой группы.

10.5.2 interfaces bridge <brx> address

Назначение адреса мостовой группе.

Синтаксис

```
set interfaces bridge <brx> address [<ip-адрес> | dhcp]
delete interfaces bridge <brx> address [<ip-адрес> | dhcp]
show interfaces bridge <brx> address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    bridge brx {
       address ip-адрес | dhcp
    }
}
```

Параметры

brx

Множественный узел. Идентификатор мостовой группы. Значение должно лежать в диапазоне от br0 до br999.

ip-адрес

IPv4-адрес или IPv6-адрес для данной мостовой группы. Допустимые значения представлены в таблице ниже:

Таблица 40 – Формат указания ip-адреса для интерфейса

Значение	Описание
<x.x.x.x/x>	IPv4-адрес/префикс (например: 192.168.10.254/24).
<h:h:h:h:h:h:h:h/x>	IPv6-адрес/префикс (например, 2001:db8:1234::/48)

Назначить мостовой группе несколько IP-адресов можно, создав соответствующее количество узлов конфигурации **address.**

dhcp

Параметр определяет мостовую группу как клиент протокола DHCP, получающий адрес и префикс от сервера DHCP.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для назначения IP-адреса мостовой группе.

Форма **set** данной команды используется для назначения адреса мостовой группе.

Форма **delete** данной команды используется для удаления настройки адреса мостовой группе.

Форма **show** данной команды используется для просмотра настройки мостовой группы.

10.5.3 interfaces bridge <brx> aging <время_хранения>

Установка интервала времени, в течение которого MAC-адрес хранится в таблице пересылки мостовой группы.

Синтаксис

```
set interfaces bridge <brx> aging <время_хранения>
delete interfaces bridge <brx> aging
show interfaces bridge <brx> aging
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bridge brx {
      aging время_хранения
   }
}
```

Параметры

brx

Множественный узел. Идентификатор мостовой группы. Значение должно лежать в диапазоне от br0 до br999.

время_хранения

Интервал времени хранения, в секундах, по истечении которого MAC-адрес удаляется из таблицы пересылки. Значение должно лежать в диапазоне от 0 до 4294967295.

Значение по умолчанию

MAC-адрес удаляется из таблицы адресов через 300 секунд (5 минут).

Указания по использованию

Команда используется для указания времени, в течение которого MAC-адрес хранится в таблице пересылки моста. Если в течение данного интервала времени запись в таблице не обновляется, она считается устаревшей, после чего удаляется из таблицы.

Форма **set** данной команды используется для установки времени хранения MAC-адреса в таблице пересылки сетевого моста.

Форма **delete** данной команды используется для восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настроек времени хранения MAC-адресов в таблице пересылки сетевого моста.

10.5.4 interfaces bridge <brx> description <описание>

Текстовое описание мостовой группы.

Синтаксис

```
set interfaces bridge <brx> description <описание>
delete interfaces bridge <brx> description
show interfaces bridge <brx> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bridge brx {
      description описание
   }
}
```

Параметры

brx

Множественный узел. Идентификатор мостовой группы. Значение должно лежать в диапазоне от br0 до br999.

описание

Мнемоническое имя или описание мостовой группы.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для создания текстового описания мостовой группы.

Форма **set** данной команды используется для создания тестового описания мостовой группы.

Форма **delete** данной команды используется для удаления текстового описания мостовой группы.

Форма **show** данной команды используется для просмотра настроек описания мостовой группы.

10.5.5 interfaces bridge <brx> disable

Отключение мостовой группы с сохранением настройки.

Синтаксис

```
set interfaces bridge <brx> disable
delete interfaces bridge <brx> disable
show interfaces bridge <brx>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bridge brx {
      disable
   }
}
```

Параметры

brx

Множественный узел. Идентификатор мостовой группы. Значение должно лежать в диапазоне от br0 до br999.

Значение по умолчанию

Мост включен.

Указания по использованию

Команда используется для отключения мостовой группы.

Форма **set** данной команды используется для отключения моста на интерфейсе.

Форма **delete** данной команды используется для восстановления мостовой группы.

Форма **show** данной команды используется для просмотра настройки мостовой группы.

10.5.6 interfaces bridge <brx> enable-proxy-arp

Включение режима проксирования ARP для мостовой группы.

Синтаксис

```
set interfaces bridge <brx> enable-proxy-arp
delete interfaces bridge <brx> enable-proxy-arp
show interfaces bridge <brx>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bridge brx {
      enable-proxy-arp
   }
}
```

Параметры

brx

Множественный узел. Идентификатор мостовой группы. Значение должно лежать в диапазоне от br0 до br999.

Значение по умолчанию

Режим проксирования ARP для мостовой группы отключен.

Указания по использованию

Команда используется для включения режима проксирования ARP для мостовой группы.

Режим проксирования ARP позволяет мостовой группе отвечать на запросы ARP (используя свой собственный MAC-адрес) в том случае, если IP-адрес назначения принадлежит подсетям, подключенным к другим интерфейсам системы. Последующие пакеты для данного IP-адреса назначения будут соответствующим образом перенаправляться системой.

Форма **set** данной команды используется для включения режима проксирования.

Форма **delete** данной команды используется для восстановления поведения, принятого по умолчанию.

Форма **show** данной команды используется для просмотра настройки.

10.5.7 interfaces bridge <brx> forwarding-delay <время_задержки>

Установка времени задержки пересылки, в течение которого мостовая группа продолжает прослушивание после изменения топологии.

Синтаксис

```
set interfaces bridge <brx> forwarding-delay <время_задержки>
delete interfaces bridge <brx> forwarding-delay
show interfaces bridge <brx> forwarding-delay
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bridge brx {
      forwarding-delay время_задержки
   }
}
```

Параметры

brx

Множественный узел. Идентификатор мостовой группы. Значение должно лежать в диапазоне от br0 до br999.

время_задержки

Интервал времени, в секундах, в течение которого мостовая группа находится в состоянии прослушивания сведений о топологии связующего дерева после изменения топологии. Значение должно лежать в диапазоне от 2 до 30.

Значение по умолчанию

Перед переходом в режим пересылки мостовая группа находится в состоянии прослушивания в течение 15 секунд.

Указания по использованию

Команда используется для установки интервала времени, в течение которого мостовая группа находится в состоянии прослушивания после изменения топологии.

После изменения топологии сети мостовая группа остается в режиме прослушивания на время задержки пересылки, получая в течение этого интервала времени сведения о топологии связующего дерева. В течение этого интервала времени сетевой трафик не пересылается. После истечения интервала задержки пересылки мостовая группа переходит в режим пересылки и возобновляет пересылку трафика.

Форма **set** данной команды используется для установки времени задержки пересылки.

Форма **delete** данной команды используется для восстановления длительности интервала задержки пересылки до его значения, принятого по умолчанию.

Форма **show** данной команды используется для просмотра настройки времени задержки пересылки.

10.5.8 interfaces bridge <brx> max-age <интервал>

Установка времени ожидания мостовой группой пакета "hello" от корня связующего дерева.

Синтаксис

```
set interfaces bridge <brx> max-age <интервал>
delete interfaces bridge <brx> max-age
show interfaces bridge <brx> max-age
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bridge brx {
      max-age интервал
   }
}
```

Параметры

brx

Множественный узел. Идентификатор мостовой группы. Значение должно лежать в диапазоне от br0 до br999.

интервал

Интервал времени, в секундах, в течение которого мостовая группа ожидает получения пакета "hello" перед перевычислением топологии связующего дерева. Значение должно лежать в диапазоне от 6 до 40.

Значение по умолчанию

Мостовая группа в течение 20 секунд ожидает получения пакетов "hello" перед перевычислением топологии связующего дерева.

Указания по использованию

Команда используется для установки интервала, в течение которого мостовая группа ожидает получения пакетов "hello" от корня связующего дерева. Если в течение этого интервала мостовая группа не получает пакета "hello", считается, что топология сети изменилась, после чего топология связующего дерева вычисляется заново.

Форма **set** данной команды используется для установки интервала ожидания пакета "hello".

Форма **delete** данной команды используется для восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настроек интервала ожидания пакета "hello".

10.5.9 interfaces bridge <brx> hello-time <интервал>

Интервал времени, через который мостовая группа отправляет пакет "hello".

Синтаксис

```
set interfaces bridge <brx> hello-time <интервал>
delete interfaces bridge <brx> hello-time
show interfaces bridge <brx> hello-time
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bridge brx {
```

```
        hello-time интервал
    }
}
```

Параметры

brx

Множественный узел. Идентификатор мостовой группы. Значение должно лежать в диапазоне от br0 до br999.

интервал

Интервал времени, в секундах, через который данная мостовая группа будет передавать пакеты "hello". Значение должно лежать в диапазоне от 1 до 10. Значение по умолчанию равно 2.

Значение по умолчанию

Передача пакетов осуществляется каждые 2 секунды.

Указания по использованию

Команда используется для установки интервала времени, через который мостовая группа посылает пакеты "hello". Пакеты "hello" представляют собой блоки BPDU (Bridge Protocol Data Units), которые используются для передачи информации о структуре топологии сети.

В связующем дереве пакеты "hello" отправляются мостовой группой, которая принимает на себя роль корневого моста.

Форма **set** данной команды используется для установки интервала передачи пакетов "hello".

Форма **delete** данной команды используется для восстановления длительности интервала передачи пакетов "hello", принятого по умолчанию.

Форма **show** данной команды используется для просмотра настроек интервала передачи пакетов "hello".

10.5.10 interfaces bridge <brx> priority <приоритет>

Установка приоритета пересылки для мостовой группы в связующем дереве.

Синтаксис

```
set interfaces bridge <brx> priority <приоритет>
delete interfaces bridge <brx> priority
show interfaces bridge <brx> priority
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bridge brx {
       priority приоритет
  }
}
```

Параметры

brx

Множественный узел. Идентификатор мостовой группы. Значение должно лежать в диапазоне от br0 до br999.

приоритет

Приоритет пересылки мостовой группы в рамках связующего дерева. Чем меньше установленное значение, тем больший приоритет имеет мостовая группа. Значение должно лежать в диапазоне от 0 до 65535.

Значение по умолчанию

Значение по умолчанию равно 32768.

Указания по использованию

Команда используется для установки приоритета пересылки данной мостовой группы в структуре связующего дерева.

Значение приоритета учитывается при выборе корня связующего дерева. Чем меньше значение, назначенное мостовой группе, тем выше ее приоритет и тем больше вероятность того, что данная мостовая группа будет выбрана в качестве корня связующего дерева.

Форма **set** данной команды используется для установки приоритета данного моста в связующем дереве.

Форма **delete** данной команды используется для восстановления приоритета, принятого по умолчанию.

Форма **show** данной команды используется для просмотра настройки приоритета.

10.5.11 interfaces bridge <brx> stp <состояние>

Включение протокола STP (IEEE 802.1D Spanning Tree Protocol) для мостовой группы.

Синтаксис

```
set interfaces bridge <brx> stp <состояние>
delete interfaces bridge <brx> stp
show interfaces bridge <brx> stp
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bridge brx {
      stp состояние
   }
}
```

Параметры

brx

Множественный узел. Идентификатор мостовой группы. Значение должно лежать в диапазоне от br0 до br999.

состояние

Позволяет включить или отключить протокол STP для указанной мостовой группы. Допустимые значения представлены ниже:

true: Включение протокола STP для данной мостовой группы.

false: Выключение протокола STP для данной мостовой группы.

Значение по умолчанию

Протокол STP выключен.

Указания по использованию

Команда используется для включения и выключения протокола STP (Spanning Tree Protocol) для указанной мостовой группы. Если для мостовой группы включен протокол STP, он функционирует на всех (в том числе виртуальных) интерфейсах, входящих в состав данной мостовой группы.

Форма **set** данной команды используется для включения протокола STP для данной мостовой группы.

Форма **delete** данной команды используется для отключения протокола STP для данной мостовой группы.

Форма **show** данной команды используется для отображения настроек.

10.5.12 interfaces ethernet <ethx> bridge-group bridge <brx>

Включение интерфейса Ethernet в состав мостовой группы.

Синтаксис

```
set interfaces ethernet <ethx> bridge-group bridge <brx>
delete interfaces ethernet <ethx> bridge-group bridge
show interfaces ethernet <ethx> bridge-group bridge
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      bridge-group {
         bridge brx
      }
   }
}
```

Параметры

ethx

Множественный узел. Интерфейс Ethernet, который требуется включить в состав мостовой группы. Интерфейс должен быть заранее определен. Значение должно лежать в диапазоне от eth0 до eth999 в зависимости от реально имеющихся в системе интерфейсов Ethernet.

brx

Множественный узел. Идентификатор мостовой группы. Значение должно лежать в диапазоне от br0 до br999.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для включения интерфейса Ethernet в состав мостовой группы.

Форма **set** данной команды используется для включения интерфейса Ethernet в состав мостовой группы.

Форма **delete** данной команды используется для исключения интерфейса Ethernet из состава мостовой группы.

Форма **show** данной команды используется для вывода сведений об интерфейсах Ethernet, входящих в состав мостовой группы.

10.5.13 interfaces ethernet <ethx> bridge-group cost <стоимость>

Установка стоимости пути для интерфейса Ethernet, входящего в состав мостовой группы.

Синтаксис

```
set interfaces ethernet <ethx> bridge-group cost <стоимость>
delete interfaces ethernet <ethx> bridge-group cost
show interfaces ethernet <ethx> bridge-group cost
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
```

```
    ethernet ethx {
        bridge-group {
            cost стоимость
        }
    }
}
```

Параметры

ethx

Множественный узел. Интерфейс Ethernet, который требуется включить в состав мостовой группы. Интерфейс должен быть заранее определен. Значение должно лежать в диапазоне от eth0 до eth999 в зависимости от реально имеющихся в системе интерфейсов Ethernet.

стоимость

Стоимость пути для интерфейса, входящего в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 65535.

Значение по умолчанию

Значение по умолчанию для стоимости пути рассчитывается исходя из пропускной способности канала. Ниже приведена таблица соответствия пропускной способности и назначаемой по умолчанию стоимости пути.

Таблица 41 – Таблица соответствия пропускной способности

Пропускная способность канала	Стоимость пути протокола STP для интерфейса
4 Mbit/s	250
10 Mbit/s	100
16 Mbit/s	62
100 Mbit/s	19
1 Gbit/s	4
2 Gbit/s	3
10 Gbit/s	2

Указания по использованию

Команда используется при установке стоимости пути для интерфейса, входящего в состав мостовой группы. Протокол STP использует это значение для вычисления кратчайшего пути от данной мостовой группы до корня связующего дерева.

Форма **set** данной команды используется для установки стоимости пути.

Форма **delete** данной команды используется для восстановления значения стоимости пути, принятого по умолчанию.

Форма **show** данной команды используется для просмотра сведений о настройке стоимости пути для интерфейса.

10.5.14 interfaces ethernet <ethx> bridge-group priority <приоритет>

Установка приоритета для интерфейса Ethernet, входящего в состав мостовой группы.

Синтаксис

```
set interfaces ethernet <ethx> bridge-group priority <приоритет>
delete interfaces ethernet <ethx> bridge-group priority
show interfaces ethernet <ethx> bridge-group priority
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
```

```
    ethernet ethx {
        bridge-group {
            priority приоритет
        }
    }
}
```

Параметры

ethx

Множественный узел. Интерфейс Ethernet, который требуется включить в состав мостовой группы. Интерфейс должен быть заранее определен. Значение должно лежать в диапазоне от eth0 до eth999 в зависимости от реально имеющихся в системе интерфейсов Ethernet.

приоритет

Приоритет для интерфейса, входящего в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 63.

Значение по умолчанию

Приоритет равен 32.

Указания по использованию

Команда позволяет установить приоритет для интерфейса Ethernet, входящего в состав мостовой группы, что определяет предпочтительность того или иного пути.

Форма **set** данной команды используется для установки приоритета пути.

Форма **delete** данной команды используется для восстановления значения приоритета пути, принятого по умолчанию.

Форма **show** данной команды используется для просмотра настройки приоритета пути для интерфейса.

10.5.15 interfaces ethernet <ethx> vif <идентификатор_vlan> bridge-group bridge <brx>

Включение виртуального интерфейса в состав мостовой группы.

Синтаксис

```
set interfaces ethernet <ethx> vif <идентификатор_vlan> bridge-group bridge <brx>

delete interfaces ethernet <ethx> vif <идентификатор_vlan> bridge-group bridge

show interfaces ethernet <ethx> vif <идентификатор_vlan> bridge-group bridge
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    ethernet ethx {
        vif идентификатор_vlan {
            bridge-group {
                bridge brx
            }
        }
    }
}
```

Параметры

ethx

Множественный узел. Интерфейс Ethernet, на базе которого создан виртуальный интерфейс. Интерфейс должен быть заранее определен. Значение должно лежать в диапазоне от eth0 до eth999 в зависимости от реально имеющихся в системе интерфейсов Ethernet.

идентификатор_vlan

Множественный узел. Идентификатор виртуального интерфейса, который требуется включить в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 4094. Виртуальный интерфейс должен быть заранее определен.

brx

Множественный узел. Идентификатор мостовой группы, в состав которой требуется включить интерфейс. Значение должно лежать в диапазоне от br0 до br999.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для включения виртуального интерфейса Ethernet в состав мостовой группы.

Форма **set** данной команды используется включения виртуального интерфейса в состав мостовой группы.

Форма **delete** данной команды используется для исключения виртуального интерфейса из состава мостовой группы.

Форма **show** данной команды используется для просмотра сведений о виртуальных интерфейсах, входящих в состав мостовой группы.

10.5.16 interfaces ethernet <ethx> vif <идентификатор_vlan> bridge-group cost <стоимость>

Установка стоимости пути для виртуального интерфейса Ethernet, входящего в состав мостовой группы.

Синтаксис

```
set interfaces ethernet <ethx> vif <идентификатор_vlan> bridge-group cost <стоимость>
delete interfaces ethernet <ethx> vif <идентификатор_vlan> bridge-group cost
show interfaces ethernet <ethx> vif <идентификатор_vlan> bridge-group cost
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    ethernet ethx {
        vif идентификатор_vlan {
            bridge-group {
                cost стоимость
            }
        }
    }
}
```

Параметры

ethx

Множественный узел. Интерфейс Ethernet, на базе которого создан виртуальный интерфейс. Интерфейс должен быть заранее определен. Значение должно лежать в диапазоне от eth0 до eth999 в зависимости от реально имеющихся в системе интерфейсов Ethernet.

идентификатор_vlan

Множественный узел. Идентификатор виртуального интерфейса, который требуется включить в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 4094. Виртуальный интерфейс должен быть заранее определен.

стоимость

Стоимость пути для виртуального интерфейса, входящего в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 65535.

Значение по умолчанию

Значение по умолчанию для стоимости пути рассчитывается исходя из пропускной способности канала. Ниже приведена таблица соответствия пропускной способности и назначаемой по умолчанию стоимости пути.

Таблица 42 – Соответсвие пропускной способности канала

Пропускная способность канала	Стоимость пути протокола STP для интерфейса
4 Mbit/s	250
10 Mbit/s	100
16 Mbit/s	62
100 Mbit/s	19
1 Gbit/s	4
2 Gbit/s	3
10 Gbit/s	2

Указания по использованию

Команда позволяет установить стоимость пути для виртуального интерфейса Ethernet, входящего в состав мостовой группы. Протокол STP использует это значение для вычисления кратчайшего пути от данной мостовой группы до корня связующего дерева.

Форма **set** данной команды используется для установки стоимости пути.

Форма **delete** данной команды используется для восстановления значения стоимости пути, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки стоимости пути.

10.5.17 interfaces ethernet <ethx> vif <идентификатор_vlan> bridge-group priority <приоритет>

Установка приоритета для виртуального интерфейса Ethernet, входящего в состав мостовой группы.

Синтаксис

```
set interfaces ethernet <ethx> vif <идентификатор_vlan> bridge-group priority
<приоритет>

delete interfaces ethernet <ethx> vif <идентификатор_vlan> bridge-group
priority

show interfaces ethernet <ethx> vif <идентификатор_vlan> bridge-group
priority
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      vif идентификатор_vlan {
         bridge-group {
            priority приоритет
         }
      }
   }
}
```

Параметры

ethx

Множественный узел. Интерфейс Ethernet, на базе которого создан виртуальный интерфейс. Интерфейс должен быть заранее определен. Значение должно лежать в диапазоне от eth0 до eth999 в зависимости от реально имеющихся в системе интерфейсов Ethernet.

идентификатор_vlan

Множественный узел. Идентификатор виртуального интерфейса, который требуется включить в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 4094. Виртуальный интерфейс должен быть заранее определен.

приоритет

Приоритет для виртуального интерфейса, входящего в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 63.

Значение по умолчанию

Приоритет равен 32.

Указания по использованию

Команда позволяет установить приоритет для виртуального интерфейса, входящего в состав мостовой группы.

Форма **set** данной команды используется для установки приоритета пути.

Форма **delete** данной команды используется для восстановления значения приоритета пути, принятого по умолчанию.

Форма **show** данной команды используется для просмотра настройки приоритета пути.

10.5.18 interfaces bonding <bondx> bridge-group bridge <brx>

Включение интерфейса агрегированных каналов Ethernet в состав мостовой группы.

Синтаксис

```
set interfaces bonding <bondx> bridge-group bridge <brx>
delete interfaces bonding <bondx> bridge-group bridge
show interfaces bonding <bondx> bridge-group bridge
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bonding bondx {
      bridge-group {
```

```
            bridge brx
        }
    }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet. Интерфейс должен быть заранее определен. Значение должно лежать в диапазоне от bond0 до bond99.

brx

Множественный узел. Идентификатор мостовой группы, в состав которой требуется включить интерфейс. Значение должно лежать в диапазоне от br0 до br999.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для включения интерфейса агрегированных каналов Ethernet в состав мостовой группы.

Форма **set** этой команды используется для включения интерфейса агрегированных каналов Ethernet в состав мостовой группы.

Форма **delete** этой команды используется для исключения интерфейса агрегированных каналов Ethernet из состава мостовой группы.

Форма **show** этой команды используется для отображения информации об интерфейсах агрегированных каналов Ethernet, входящих в состав мостовой группы.

10.5.19 interfaces bonding <bondx> bridge-group cost <стоимость>

Установка стоимости пути для интерфейса агрегированных каналов Ethernet, входящего в состав мостовой группы.

Синтаксис

```
set interfaces bonding <bondx> bridge-group cost <стоимость>
delete interfaces bonding <bondx> bridge-group cost
show interfaces bonding <bondx> bridge-group cost
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    bonding bondx {
        bridge-group {
            cost стоимость
        }
    }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet. Интерфейс должен быть заранее определен. Значение должно лежать в диапазоне от bond0 до bond99.

стоимость

Стоимость пути для интерфейса агрегированных каналов, входящего в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 65535.

Значение по умолчанию

Значение по умолчанию для стоимости пути рассчитывается исходя из пропускной способности канала. Ниже приведена таблица соответствия пропускной способности и назначаемой по умолчанию стоимости пути.

Таблица 43 – Таблица пропускной способности

Пропускная способность канала	Стоимость пути протокола STP для интерфейса
4 Mbit/s	250
10 Mbit/s	100
16 Mbit/s	62
100 Mbit/s	19
1 Gbit/s	4
2 Gbit/s	3
10 Gbit/s	2

Указания по использованию

Команда позволяет установить стоимость пути для интерфейса агрегированных каналов, входящего в состав мостовой группы. Протокол STP использует это значение для вычисления кратчайшего пути от данной мостовой группы до корня связующего дерева.

Форма **set** данной команды используется для установки стоимости пути.

Форма **delete** данной команды используется для восстановления значения стоимости пути, принятого по умолчанию.

Форма **show** данной команды используется для просмотра сведений о настройке стоимости пути для интерфейса.

10.5.20 interfaces bonding <bondx> bridge-group priority <приоритет>

Установка приоритета для интерфейса агрегированных каналов Ethernet, входящего в состав мостовой группы.

Синтаксис

```
set interfaces bonding <bondx> bridge-group priority <приоритет>
delete interfaces bonding <bondx> bridge-group priority
show interfaces bonding <bondx> bridge-group priority
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bonding bondx {
      bridge-group {
         priority приоритет
      }
   }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet. Интерфейс должен быть заранее определен. Значение должно лежать в диапазоне от bond0 до bond99.

приоритет

Приоритет для интерфейса агрегированных каналов, входящего в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 63.

Значение по умолчанию

Приоритет равен 32.

Указания по использованию

Команда используется для назначения приоритета для интерфейса агрегированных каналов Ethernet, входящего в состав мостовой группы.

Форма **set** данной команды используется для установки приоритета пути.

Форма **delete** данной команды используется для восстановления значения приоритета пути, принятого по умолчанию.

Форма **show** данной команды используется для просмотра настройки приоритета пути для интерфейса.

10.5.21 interfaces bonding <bondx> vif <идентификатор_vlan> bridge-group bridge <brx>

Включение виртуального интерфейса агрегированных каналов Ethernet в состав мостовой группы.

Синтаксис

```
set interfaces bonding <bondx> vif <идентификатор_vlan> bridge-group bridge <brx>

delete interfaces bonding <bondx> vif <идентификатор_vlan> bridge-group bridge

show interfaces bonding <bondx> vif <идентификатор_vlan> bridge-group bridge
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    bonding bondx {
        vif идентификатор_vlan {
            bridge-group {
                bridge brx
            }
        }
    }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet, на базе которого создан виртуальный интерфейс. Интерфейс должен быть заранее определен. Значение должно лежать в диапазоне от bond0 до bond99.

идентификатор_vlan

Множественный узел. Идентификатор виртуального интерфейса агрегированных каналов Ethernet, который требуется включить в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 4094. Виртуальный интерфейс должен быть заранее определен.

brx

Множественный узел. Идентификатор мостовой группы, в состав которой требуется включить интерфейс. Значение должно лежать в диапазоне от br0 до br999.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для включения виртуального интерфейса агрегированных каналов Ethernet в состав мостовой группы.

Форма **set** данной команды используется для включения виртуального интерфейса агрегированных каналов в состав мостовой группы.

Форма **delete** данной команды используется для исключения виртуального интерфейса агрегированных каналов из состава мостовой группы.

Форма **show** данной команды используется для отображения сведений о виртуальных интерфейсах агрегированных каналов Ethernet, входящих в состав мостовой группы.

10.5.22 interfaces bonding <bondx> vif <идентификатор_vlan> bridge-group cost <стоимость>

Установка стоимости пути для виртуального интерфейса агрегированных каналов Ethernet, входящего в состав мостовой группы.

Синтаксис

```
set interfaces bonding <bondx> vif <идентификатор_vlan> bridge-group cost <стоимость>
delete interfaces bonding <bondx> vif <идентификатор_vlan> bridge-group cost
show interfaces bonding <bondx> vif <идентификатор_vlan> bridge-group cost
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bonding bondx {
      vif идентификатор_vlan {
         bridge-group {
            cost стоимость
         }
      }
   }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet, на базе которого создан виртуальный интерфейс. Интерфейс должен быть заранее определен. Значение должно лежать в диапазоне от bond0 до bond99.

идентификатор_vlan

Множественный узел. Идентификатор виртуального интерфейса агрегированных каналов Ethernet, который требуется включить в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 4094. Виртуальный интерфейс должен быть заранее определен.

стоимость

Стоимость пути для виртуального интерфейса агрегированных каналов Ethernet, входящего в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 65535.

Значение по умолчанию

Значение по умолчанию для стоимости пути рассчитывается исходя из пропускной способности канала. Ниже приведена таблица соответствия пропускной способности и назначаемой по умолчанию стоимости пути.

Таблица 44 – Таблица пропускной способности

Пропускная способность канала	Стоимость пути протокола STP для интерфейса
4 Mbit/s	250
10 Mbit/s	100
16 Mbit/s	62
100 Mbit/s	19
1 Gbit/s	4
2 Gbit/s	3
10 Gbit/s	2

Указания по использованию

Команда позволяет установить стоимость пути для виртуального интерфейса агрегированных каналов Ethernet, входящего в состав мостовой группы. Протокол STP использует это значение для вычисления кратчайшего пути от данной мостовой группы до корня связующего дерева.

Форма **set** данной команды используется для установки стоимости пути.

Форма **delete** данной команды используется для восстановления значения стоимости пути, принятого по умолчанию.

Форма **show** данной команды используется для просмотра сведений о настройке стоимости пути для интерфейса.

10.5.23 interfaces bonding <bondx> vif <идентификатор_vlan> bridge-group priority <приоритет>

Установка приоритета для виртуального интерфейса агрегированных каналов Ethernet, входящего в состав мостовой группы.

Синтаксис

```
set interfaces bonding <bondx> vif <идентификатор_vlan> bridge-group priority <приоритет>
```

```
delete interfaces bonding <bondx> vif <идентификатор_vlan> bridge-group priority
```

```
show interfaces bonding <bondx> vif <идентификатор_vlan> bridge-group priority
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bonding bondx {
     vif идентификатор_vlan {
         bridge-group {
            priority приоритет
         }
     }
   }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet, на базе которого создан виртуальный интерфейс. Интерфейс должен быть заранее определен. Значение должно лежать в диапазоне от bond0 до bond99.

идентификатор_vlan

Множественный узел. Идентификатор виртуального интерфейса агрегированных каналов Ethernet, который требуется включить в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 4094. Виртуальный интерфейс должен быть заранее определен.

приоритет

Приоритет для виртуального интерфейса агрегированных каналов Ethernet, входящего в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 63.

Значение по умолчанию

Приоритет равен 32.

Указания по использованию

Команда позволяет назначить приоритет для виртуального интерфейса агрегированных каналов Ethernet, входящего в состав мостовой группы.

Форма **set** данной команды используется для установки приоритета пути.

Форма **delete** данной команды используется для восстановления значения приоритета пути, принятого по умолчанию.

Форма **show** данной команды используется для просмотра настройки приоритета пути для интерфейса.

10.5.24 interfaces tunnel <tunx> bridge-group bridge <brx>

Включение туннельного интерфейса GRE в состав мостовой группы.

Синтаксис

```
set interfaces tunnel <tunx> bridge-group bridge <brx>
delete interfaces tunnel <tunx> bridge-group bridge
show interfaces tunnel <tunx> bridge-group bridge
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   tunnel tunx {
      bridge-group {
         bridge brx
      }
   }
}
```

Параметры

tunx

Множественный узел. Идентификатор туннельного интерфейса GRE. Интерфейс должен быть заранее определен. Поддерживаются значения в диапазоне от tun0 до tun999.

brx

Множественный узел. Идентификатор мостовой группы, в состав которой требуется включить интерфейс. Значение должно лежать в диапазоне от br0 до br999.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для включения туннельного интерфейса GRE в состав мостовой группы.

ПРИМЕЧАНИЕ В состав сетевого моста могут быть включены только туннели GRE специального типа, созданные с использованием параметра **gre-bridge**. Туннели GRE такого типа должны быть использованы только в тех случаях, когда туннельные интерфейсы требуется включить в состав мостовой группы.

Форма **set** данной команды используется для включения туннельного интерфейса GRE в состав мостовой группы.

Форма **delete** данной команды используется для исключения туннельного интерфейса GRE из состава мостовой группы.

Форма **show** данной команды используется для отображения сведений о туннельных интерфейсах GRE, входящих в состав мостовой группы.

10.5.25 interfaces tunnel <tunx> bridge-group cost <стоимость>

Установка стоимости пути для туннельного интерфейса GRE, входящего в состав мостовой группы.

Синтаксис

```
set interfaces tunnel <tunx> bridge-group cost <стоимость>
delete interfaces tunnel <tunx> bridge-group cost
show interfaces tunnel <tunx> bridge-group cost
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   tunnel tunx {
      bridge-group {
         cost стоимость
      }
   }
}
```

Параметры

tunx

Множественный узел. Идентификатор туннельного интерфейса GRE. Интерфейс должен быть заранее определен. Поддерживаются значения в диапазоне от tun0 до tun999.

стоимость

Стоимость пути для туннельного интерфейса GRE, входящего в состав мостовой группы. Значение должно лежать в диапазоне от 1 до 65535.

Значение по умолчанию

Значение по умолчанию для стоимости пути рассчитывается исходя из пропускной способности канала. Ниже приведена таблица соответствия пропускной способности и назначаемой по умолчанию стоимости пути.

Таблица 45 – Таблица пропускной способности

Пропускная способность канала	Стоимость пути протокола STP для интерфейса
4 Mbit/s	250
10 Mbit/s	100

16 Mbit/s	62
100 Mbit/s	19
1 Gbit/s	4
2 Gbit/s	3
10 Gbit/s	2

Указания по использованию

Команда позволяет установить стоимость пути для туннельного интерфейса GRE, входящего в состав мостовой группы. Протокол STP использует это значение для вычисления кратчайшего пути от данной мостовой группы до корня связующего дерева.

Форма **set** данной команды используется для установки стоимости пути.

Форма **delete** данной команды используется для восстановления значения стоимости пути, принятого по умолчанию.

Форма **show** данной команды используется для просмотра сведений о настройке стоимости пути для интерфейса.

10.5.26 interfaces tunnel <tunx> bridge-group priority <приоритет>

Установка приоритета для туннельного интерфейса GRE, входящего в состав мостовой группы.

Синтаксис

```
set interfaces tunnel <tunx> bridge-group priority <приоритет>
delete interfaces tunnel <tunx> bridge-group priority
show interfaces tunnel <tunx> bridge-group priority
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   tunnel tunx {
      bridge-group {
         priority приоритет
      }
   }
}
```

Параметры

tunx

Множественный узел. Идентификатор туннельного интерфейса GRE. Интерфейс должен быть заранее определен. Поддерживаются значения в диапазоне от tun0 до tun999.

приоритет

Приоритет для туннельного интерфейса GRE, входящего в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 63.

Значение по умолчанию

Приоритет равен 32.

Указания по использованию

Команда позволяет назначить приоритет для туннельного интерфейса GRE, входящего в состав мостовой группы.

Форма **set** данной команды используется для установки приоритета пути.

Форма **delete** данной команды используется для восстановления значения приоритета пути, принятого по умолчанию.

Форма **show** данной команды используется для просмотра настройки приоритета пути для интерфейса.

10.5.27 clear interfaces bridge counters

Очистка статистической информации для интерфейса моста.

Синтаксис

```
clear interfaces bridge [<brx>] counters
```

Режим интерфейса

Эксплуатационный режим.

Параметры

brx

Идентификатор мостовой группы, для которого требуется очистить счетчики.

Значение по умолчанию

Статистические счетчики очищаются для всех мостовых интерфейсов.

Указания по использованию

Команда используется для очистки статистических счетчиков для мостовой группы. Если идентификатор мостовой группы явно не указан, статистические счетчики очищаются для всех мостовых групп. Просмотреть значения счетчиков можно при помощи команды **show interfaces counters**.

10.5.28 show bridge

Вывод сведений об активных мостовых группах.

Синтаксис

```
show bridge [<brx> [macs | spanning-tree]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

brx

Идентификатор мостовой группы. Отображение сведений для указанной мостовой группы.

macs

Отображение таблицы MAC-адресов указанной мостовой группы.

spanning-tree

Сведения о связующем дереве для указанной мостовой группы.

Указания по использованию

Команда используется для отображения информации о настроенных сетевых мостах.

При использовании без параметров сведения выводятся для всех активных мостовых групп. Если указан идентификатор мостовой группы, сведения отображаются только для указанной мостовой группы.

Команда позволяет отобразить таблицу MAC-адресов и связанные с протоколом STP сведения для мостовой группы.

Примеры

В примере ниже выводятся сведения о настройках протокола STP для мостовой группы br0 системы edge.

Пример 101– Отображение сведений о настройках протокола STP

```
admin@edge:~$ show bridge br0 spanning-tree
```

```
br0
 bridge id               8000.000000000000
 designated root         8000.000000000000
 root port                  0                    path cost                  0
 max age                   20.00                 bridge max age
20.00
 hello time                 2.00                 bridge hello time
2.00
 forward delay             15.00                 bridge forward delay
15.00
 ageing time              300.00
 hello timer                0.00                 tcn timer
0.00
 topology change timer      0.00                 gc timer
200.55
 flags


admin@edge:~$
```

10.5.29 show interfaces bridge

Вывод сведений об интерфейсе сетевого моста.

Синтаксис

```
show interfaces bridge [ detail | <brx> [brief | capture [not port <порт> | port <порт>] | queue [class | filter]]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

detail

Отображение подробных сведений о мостовых группах.

brx

Идентификатор мостовой группы. Отображение сведений для указанной мостовой группы.

brief

Отображение кратких сведений для указанной мостовой группы.

capture

Перехват и отображение трафика на указанной мостовой группе.

not port *порт*

Отображение сетевого трафика, записанного на всех портах, кроме указанного.

port *порт*

Отображение сетевого трафика, записанного на указанном порту.

queue

Отображение сведений об очередях для мостовой группы.

class

Отображение классов очередей для указанной мостовой группы.

filter

Отображение фильтров очередей для указанной мостовой группы.

Указания по использованию

Команда используется для вывода сведений о настроенных мостовых группах.

При использовании команды без параметров отображаются сведения обо всех настроенных мостовых группах. Если указан идентификатор мостовой группы, сведения отображаются только для указанной мостовой группы.

10.6 Агрегирование каналов Ethernet

В данном разделе описаны способы агрегирования каналов Ethernet в более крупный виртуальный канал. В данном разделе рассматриваются следующие вопросы:

- Обзор агрегирования каналов Ethernet
- Пример настройки агрегирования каналов Ethernet
- Пример настройки агрегирования каналов Ethernet с VLAN

Обзор агрегирования каналов Ethernet

В некоторых ситуациях, встречающихся при эксплуатации, имеет смысл сгруппировать несколько физических каналов для создания более крупного виртуального канала. Такая группировка позволяет увеличить пропускную способность связи между двумя устройствами без расходов на физический канал с более высокой скоростью передачи, а также обеспечить избыточность, которая позволит поддерживать связь в случае отказа одного из каналов. В области глобальных сетей для группировки нескольких каналов служит многоканальный протокол "точка-точка" (MLPPP); в области локальных сетей для группировки нескольких каналов Ethernet служит агрегирование каналов Ethernet.

С целью стандартизации была выработана спецификация IEEE 802.3ad (теперь называемая IEEE 802.1ax). Стандарт IEEE 802.3ad принят в той или иной степени всеми производителями. В этом стандарте указаны общие свойства канала, а также дано определения протокола контроля за агрегированием каналов (Link Aggregation Control Protocol, LACP).

Протокол LACP спецификации 802.3ad является активным протоколом, работающим на каналах Ethernet, настроенных для агрегирования. Данный протокол позволяет равноправным узлам обмениваться информацией для автоматического агрегирования нескольких каналов и помогает определить ситуации, когда на одной стороне отсутствует правильная настройка для агрегирования каналов. Кроме того, протокол LACP активно проверяет каждое из физических подключений между каждой парой устройств, так что удается определять отказы каналов, даже если к каждому концу канала подключены другие физические устройства (например, преобразователи физического носителя), которые в противном случае не показали бы состояние неработоспособности канала, если отказ происходит в середине физического канала. Если происходит отказ канала, трафик просто перераспределяется динамически по оставшимся каналам.

В стандарте предполагается, что все физические каналы являются полнодуплексными подключениями типа "точка-точка". Нарушение режима дуплексности или типа подключения может привести к непредсказуемому поведению агрегированного канала.

В стандарте 802.3ad указывается, что все пакеты, принадлежащие "диалогу", должны проходить по одному и тому же физическому каналу, и что дублирование пакетов не допускается. Однако, как абстракция "диалога", так и алгоритм назначения диалогов каждому каналу не специфицированы полностью; в результате конкретные реализации могут отличаться друг от друга, даже на разных концах агрегированного виртуального канала. Это может привести к асимметрии потока трафика.

Число каналов, которые могут быть агрегированы, ограничивается объемом ресурсов системы, особенно объемом ОЗУ. Каналы Ethernet в агрегированном канале не обязаны работать на одной и той же скорости.

В момент добавления к агрегированному каналу физические каналы не обязаны быть работоспособными. Что касается настройки агрегированного канала, от группы наследуется только максимальная длина передаваемого пакета (MTU). Это значит, что если изменить параметр MTU агрегированного канала, то параметр MTU нижележащих каналов Ethernet будет переопределен. Оставшаяся часть настройки всегда берется из настройки, указанной для отдельного канала Ethernet.

Пример настройки агрегирования каналов Ethernet

Для настройки агрегированного канала Ethernet создается «интерфейс агрегирования», который настраивается подобно любому другому интерфейсу Ethernet. Затем для каждого интерфейса Ethernet, который должен входить в агрегированный канал, указывается группа агрегирования — то есть указывается созданный интерфейс агрегирования каналов.

На рисунке показана простая схема агрегирования каналов Ethernet, в которой агрегированный канал Ethernet состоит из двух физических каналов Ethernet. В этом примере:

- создается интерфейс агрегирования **bond0** с параметрами по умолчанию (режим 802.3ad);
- интерфейсы **eth1** и **eth2** являются физическими каналами. Они оба добавляются к интерфейсу агрегированных каналов **bond0** в качестве каналов-участников.

Следует заметить, что отдельным физическим каналам Ethernet IP-адреса не назначаются. Если любому из составляющих каналов Ethernet назначен IP-адрес, то агрегирование работать не будет.

Для определения состояния интерфейса агрегирования и его составляющих интерфейсов Ethernet используются команды **show interfaces** и **show interfaces bonding**.

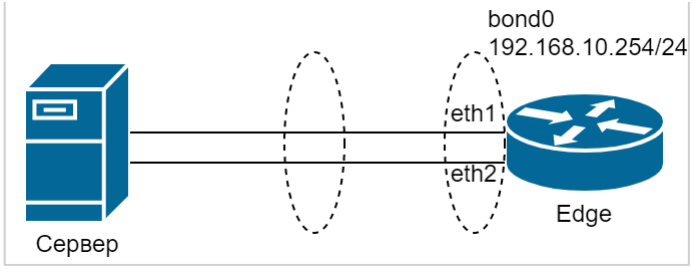


Рисунок 8 – Создание группы агрегирования из двух интерфейсов Ethernet

Для настройки данной схемы нужно выполнить следующие действия в режиме настройки.

Пример 102– Создание группы агрегирования из двух интерфейсов Ethernet

Действие	**Команда**
Создание интерфейса агрегирования каналов bond0	`[edit]` `admin@edge# set interfaces bonding bond0`
Установка IP-адреса для интерфейса агрегирования каналов	`[edit]` `admin@edge# set interfaces bonding bond0 address 192.168.10.254/24`
Добавление eth1 к интерфейсу агрегирования каналов bond0	`[edit]` `admin@edge# set interfaces ethernet eth1 bond-group bond0`
Добавление eth2 к интерфейсу агрегирования каналов bond0	`[edit]` `admin@edge# set interfaces ethernet eth2 bond-group bond0`
Фиксация изменения	`[edit]` `admin@edge# commit`

Отображение настройки интерфейса агрегирования каналов	`[edit]`
	`admin@edge# show interfaces bonding`
	`bond0 {`
	`address 192.168.10.254/24`
	`}`

Отображение настройки eth1	`[edit]`
	`admin@edge# show interfaces ethernet eth1`
	`bond-group bond0`

Отображение настройки eth2	`[edit]`
	`admin@edge# show interfaces ethernet eth2`
	`bond-group bond0`

Пример настройки агрегирования каналов Ethernet с VLAN

Если интерфейс агрегирования уже собран, становится возможным создать VLAN внутри него. В приведенном ниже примере к конфигурации из предыдущего примера добавляется VLAN. В получившемся интерфейсе агрегирования имеется как трафик VLAN, так и трафик, не относящийся к VLAN.

Для настройки данной схемы нужно выполнить следующие действия в режиме настройки.

Пример 103– Добавление VLAN к существующему интерфейсу агрегирования

Действие	**Команда**

Добавление настройки виртуального интерфейса к интерфейсу агрегирования каналов	[edit] admin@edge# set interfaces bonding bond0 vif 10 address 192.168.100.254/24
Фиксация изменения	[edit] admin@edge# commit

Отображение новой настройки интерфейса агрегирования каналов	[edit]
	admin@edge# show interfaces bonding bond0
	address 192.168.10.254/24
	vif 10 {
	address 192.168.100.254/24
	}

Команды

Команды настройки	
Группа агрегирования	
interfaces bonding <bondx>	Определение интерфейса агрегирования каналов Ethernet (группы агрегирования).
interfaces bonding <bondx> address	Назначение сетевого адреса группе агрегирования интерфейсов Ethernet.
interfaces bonding <bondx> description <описание>	Ввод описания для группы агрегирования интерфейсов Ethernet.
interfaces bonding <bondx> disable	Отключение группы агрегирования интерфейсов Ethernet с сохранением настройки.
interfaces bonding <bondx> enable-proxy-arp	Включение режима проксирования ARP для интерфейса агрегированных каналов Ethernet.
interfaces bonding <bondx> hash-mode	Установка режима режима хеширования, определяющего принцип балансировки трафика.
interfaces bonding <bondx> mac <mac-адрес>	Установка MAC-адреса группы агрегирования интерфейсов Ethernet.
interfaces bonding <bondx> mode <режим_агрегирования>	Установка режимов агрегирования для группы агрегирования интерфейсов Ethernet.
interfaces bonding <bondx> mtu <mtu>	Ввод значения MTU для группы агрегирования интерфейсов Ethernet.
interfaces bonding <bondx> primary <ethx>	Установка одного из каналов Ethernet в группе агрегирования в качестве первичного канала.
interfaces ethernet <ethx> bond-group <bondx>	Добавление интерфейса Ethernet в группу агрегирования.
Эксплуатационные команды	
show interfaces bonding	Вывод сведений о группе агрегирования интерфейсов Ethernet.

10.6.1 interfaces bonding <bondx>

Определение интерфейса агрегирования каналов Ethernet.

Синтаксис

```
set interfaces bonding <bondx>

delete interfaces bonding <bondx>

show interfaces bonding <bondx>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bonding bondx {
   }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от bond0 до bond99. Можно определить несколько групп агрегирования, создав несколько узлов конфигурации bonding.

Значение по умолчанию

Отсутствуют.

Указания по использованию

Эта команда используется для определения интерфейса агрегирования каналов Ethernet, называемого также группой агрегирования. Группа агрегирования каналов Ethernet дает возможность объединить пропускную способность отдельных каналов в единый виртуальный канал. Следует заметить, что создавать группу агрегирования (при помощи данной команды или одного из ее вариантов) нужно до назначения интерфейсов Ethernet для нее.

Форма **set** данной команды используется для определения параметров интерфейса агрегированных каналов Ethernet.

Форма **delete** данной команды используется для удаления всей настройки интерфейса агрегированных каналов Ethernet.

Форма **show** данной команды используется для просмотра настройки интерфейса агрегированных каналов Ethernet.

10.6.2 interfaces bonding <bondx> address

Назначение сетевого адреса интерфейсу агрегированных каналов Ethernet.

Синтаксис

```
set interfaces bonding <bondx> address [<ip-адрес> | dhcp]
delete interfaces bonding <bondx> address [<ip-адрес> | dhcp]
show interfaces bonding <bondx> address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bonding bondx {
      address ip-адрес | dhcp
   }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от bond0 до bond99.

ip-адрес

IPv4-адрес или IPv6-адрес для данного интерфейса агрегированных каналов Ethernet. Допустимые значения представлены в таблице ниже:

Таблица 46 – Формат указания ip-адреса для интерфейса

Значение	Описание
<x.x.x.x/x>	IPv4-адрес/префикс (например: 192.168.10.254/24).
<h:h:h:h:h:h:h:h/x>	IPv6-адрес/префикс (например, 2001:db8:1234::/48)

Назначить мостовой группе несколько IP-адресов можно, создав соответствующее количество узлов конфигурации **address.**

dhcp

Параметр определяет интерфейс агрегированных каналов Ethernet как клиент протокола DHCP, получающий адрес и префикс от сервера DHCP.

Значение по умолчанию

Отсутствуют.

Указания по использованию

Эта команда используется для установки IP-адреса и префикса подсети для группы агрегирования каналов Ethernet. С помощью параметра dhcp можно дать интерфейсу указание получать адрес и префикс от сервера DHCP.

Форма **set** этой команды используется для установки IP-адреса и префикса подсети.

Форма **delete** данной команды используется для удаления настройки IP-адреса.

Форма **show** данной команды используется для отображения настройки IP-адреса.

10.6.3 interfaces bonding <bondx> description <описание>

Ввод описания для интерфейса агрегированных каналов Ethernet.

Синтаксис

```
set interfaces bonding <bondx> description <описание>
delete interfaces bonding <bondx> description
show interfaces bonding <bondx> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bonding bondx {
      description описание
   }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от bond0 до bond99.

описание

Мнемоническое имя или описание группы агрегирования.

Значение по умолчанию

Отсутствуют.

Указания по использованию

Эта команда используется для ввода описания группы агрегирования.

Форма **set** этой команды используется для ввода описания интерфейса агрегированных каналов Ethernet.

Форма **delete** этой команды используется для удаления этого описания.

Форма **show** этой команды используется для просмотра этого описания.

10.6.4 interfaces bonding <bondx> disable

Отключение интерфейса агрегированных каналов Ethernet с сохранением настройки.

Синтаксис

```
set interfaces bonding <bondx> disable
delete interfaces bonding <bondx> disable
show interfaces bonding <bondx>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bonding bondx {
      disable
   }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от bond0 до bond99.

Значение по умолчанию

Отсутствуют.

Указания по использованию

Эта команда используется для отключения группы агрегирования каналов Ethernet без удаления настройки.

Форма **set** этой команды используется для отключения интерфейса агрегированных каналов Ethernet.

Форма **delete** этой команды используется для включения интерфейса агрегированных каналов Ethernet.

Форма **show** этой команды используется для просмотра настройки интерфейса агрегированных каналов Ethernet.

10.6.5 interfaces bonding <bondx> enable-proxy-arp

Включение режима проксирования ARP для интерфейса агрегированных каналов Ethernet.

Синтаксис

```
set interfaces bonding <bondx> enable-proxy-arp
delete interfaces bonding <bondx> enable-proxy-arp
show interfaces bonding <bondx>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bonding bondx {
      enable-proxy-arp
   }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от bond0 до bond99.

Значение по умолчанию

Режим проксирования ARP для интерфейса агрегированных каналов Ethernet отключен.

Указания по использованию

Команда используется для включения режима проксирования ARP для агрегированных каналов Ethernet.

Форма **set** данной команды используется для включения режима проксирования ARP для агрегированных каналов Ethernet.

Форма **delete** данной команды используется для восстановления поведения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки.

10.6.6 interfaces bonding <bondx> hash-mode

Установка метода хеширования, определяющего принцип балансировки трафика в режимах агрегирования xor-hash, 802.3ad и transmit-load-balance.

Синтаксис

```
set interfaces bonding <bondx> hash-mode <режим_хеширования>
delete interfaces bonding <bondx> hash-mode
show interfaces bonding <bondx>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bonding bondx {
      hash-mode <режим_хеширования>
   }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от bond0 до bond99.

режим_хеширования

Устанавливает метод хеширования, определяющий принцип балансировки трафика в режимах агрегирования xor-hash, 802.3ad и transmit-load-balance.

Таблица 47 – Допустимые методы хеширования

Значение	Описание
layer2	Хеш на основе протокола 2 уровня. Для генерации хеша используются MAC-адреса отправителя и получателя. Весь трафик между определённой парой узлов всегда идёт по определённому каналу.
layer2+3	Хеш на основе протоколов 2 и 3 уровней. Используется комбинацию MAC и IP-адресов для генерации хеша. Благодаря этому обеспечивается более равномерная балансировка трафика, особенно в случае, когда бóльшая его часть передаётся через промежуточные маршрутизаторы.
layer3+4	Хеш на основе протоколов 3 и 4 уровней. Канал для отправки пакета определяется по совокупности IP-адресов и номеров портов источника и назначения.Благодаря этому трафик определённого узла может распределяться между несколькими каналами, хотя пакеты одного и того же TCP-соединения или UDP-потока всегда передаются по одному и тому же каналу. Алгоритм не полностью совместим с IEEE 802.3ad.
encap2+3	Хеш на основе протоколов 2 и 3 уровней с разбором инкапсуляции. Используется механизм,

Значение	Описание
	аналогичный layer2+3 с возможностью анализа инкапсулированных заголовков.
encap3+4	Хеш на основе протоколов 3 и 4 уровней с разбором инкапсуляции.Используется механизм, аналогичный layer3+4 с возможностью анализа инкапсулированных заголовков.

Значение по умолчанию

По умолчанию используется метод хеширования *layer2*.

Указания по использованию

Команда используется для установки метода хеширования, определяющего принцип балансировки трафика в режимах агрегирования xor-hash, 802.3ad и transmit-load-balance.

Форма **set** этой команды используется для установки заданного метода хеширования для агрегированных каналов Ethernet.

Форма **delete** этой команды используется для удаления настроенного MAC-адреса интерфейса агрегированных каналов Ethernet.

Форма **show** этой команды используется для просмотра настройки MAC-адреса интерфейса агрегированных каналов Ethernet.

10.6.7 interfaces bonding <bondx> mac <mac-адрес>

Установка MAC-адреса интерфейса агрегированных каналов Ethernet.

Синтаксис

```
set interfaces bonding <bondx> mac <mac-адрес>

delete interfaces bonding <bondx> mac

show interfaces bonding <bondx> mac
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bonding bondx {
      mac mac-адрес
   }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от bond0 до bond99.

mac-адрес

MAC-адрес для интерфейса агрегированных каналов Ethernet. Формат должен соответствовать типу интерфейса. Для интерфейса Ethernet это шесть двузначных шестнадцатеричных чисел, разделенных двоеточиями, например 00:0a:59:9a:f2:ba.

Значение по умолчанию

В качестве MAC-адреса используется MAC-адрес первого интерфейса, добавленного в интерфейса агрегированных каналов Ethernet.

Указания по использованию

Эта команда используется для установки MAC-адреса интерфейса агрегированных каналов Ethernet.

Форма **set** этой команды используется для установки MAC-адреса интерфейса агрегированных каналов Ethernet.

Форма **delete** этой команды используется для удаления настроенного MAC-адреса интерфейса агрегированных каналов Ethernet.

Форма **show** этой команды используется для просмотра настройки MAC-адреса интерфейса агрегированных каналов Ethernet.

10.6.8 interfaces bonding <bondx> mode <режим_агрегирования>

Установка режимов агрегирования для интерфейса агрегированных каналов Ethernet.

Синтаксис

```
set interfaces bonding <bondx> mode <режим_агрегирования>
delete interfaces bonding <bondx> mode
show interfaces bonding <bondx> mode
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bonding bondx {
      mode режим_агрегирования
   }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от bond0 до bond99.

режим_агрегирования

Определяет режим агрегирования для интерфейса агрегированных каналов Ethernet. Допустимые значения представлены в таблице ниже:

Таблица 48 – Допустимые режимы агрегирования

Значение	Описание
802.3ad	Использование динамического агрегирования каналов по спецификации IEEE 802.3ad в качестве режима агрегирования. В этом режиме создаются группы агрегирования, в которых параметры скорости и режима дуплекса являются общими.
active-backup	Установка политики "активный-резервный" в качестве режима агрегирования. В этом режиме только один интерфейс Ethernet интерфейсе агрегированных каналов Ethernet (первичный, primary) является активным. Другой интерфейс Ethernet становится активным если и только если происходит сбой первичного интерфейса Ethernet. MAC-адрес интерфейса агрегирования виден снаружи только на активном интерфейсе Ethernet.
adaptive-load-balance	Использование адаптивной балансировки нагрузки в качестве режима агрегирования. В этом режиме для трафика IPv4 производятся как адаптивная балансировка нагрузки при передаче, так и балансировка нагрузки при приеме, а никакая поддержка специальным коммутатором не требуется. Балансировка нагрузки при приеме достигается с помощью согласования по протоколу ARP.
round-robin	Использование циклического перебора в качестве режима агрегирования. В этом режиме система передает пакеты с циклическим перебором интерфейсов начиная с первого доступного интерфейса Ethernet в интерфейсе агрегирования вплоть до последнего. Балансировка нагрузки циклическим перебором помогает управлять загрузкой сети и обеспечивать отказоустойчивость.
transmit-load-balance	Использование адаптивной балансировки нагрузки при передаче в качестве режима агрегирования. Этот режим является типом агрегирования каналов, не требующим никакой специальной поддержки коммутатором. Исходящий трафик распределяется в соответствии с текущей загрузкой (рассчитанной относительно скорости) на каждом интерфейсе Ethernet в

Значение	Описание
	интерфейсе агрегирования. Входящий трафик принимается текущим интерфейсом Ethernet. Если происходит сбой принимающего интерфейса Ethernet, происходит переход MAC-адреса сбойного интерфейса на другой интерфейс Ethernet.
xor-hash	Использование политики "исключающего ИЛИ" в качестве режима агрегирования. В этом режиме передача основана на политике контрольного суммирования передачи по умолчанию. Этот режим обеспечивает балансировку нагрузки и отказоустойчивость.
broadcast	Использование политики вещания в качестве режима агрегирования. В этом режиме система передает всё на все интерфейсы Ethernet. Этот режим обеспечивает отказоустойчивость, но не балансировку нагрузки.

Значение по умолчанию

В качестве режима агрегирования используется динамическое агрегирование каналов по спецификации IEEE 802.3ad.

Указания по использованию

Эта команда используется для установки режима агрегирования для интерфейса агрегированных каналов Ethernet.

Форма **set** этой команды используется для установки режима агрегирования интерфейса агрегированных каналов Ethernet.

Форма **delete** этой команды используется для восстановления режима агрегирования по умолчанию для интерфейса агрегированных каналов Ethernet.

Форма **show** этой команды используется для просмотра настройки режима агрегирования.

10.6.9 interfaces bonding <bondx> mtu <mtu>

Установка значения MTU для интерфейса агрегированных каналов Ethernet.

Синтаксис

```
set interfaces bonding <bondx> mtu <mtu>
delete interfaces bonding <bondx> mtu
show interfaces bonding <bondx> mtu
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bonding bondx {
      mtu mtu
   }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от bond0 до bond99.

mtu

Установка значения MTU для интерфейса агрегированных каналов Ethernet. Значение должно лежать в диапазоне от 68 до 9000.

Значение по умолчанию

По умолчанию значение MTU устанавливается равным 1500.

Указания по использованию

Эта команда используется для установки параметра MTU (максимальная длина передаваемого блока) для интерфейса агрегированных каналов Ethernet.

Следует заметить, в результате изменения параметра MTU для интерфейса агрегированных каналов Ethernet изменяются параметры MTU всех интерфейсов Ethernet, входящих в состав интерфейса агрегированных каналов Ethernet.

При перенаправлении пакеты IPv4, имеющие размер больший, чем значение MTU, будут фрагментированы, за исключением случая, когда установлен флаг DF. В этом случае пакеты будут проигнорированы.

Форма **set** этой команды используется для установки параметра MTU интерфейса агрегированных каналов Ethernet.

Форма **delete** этой команды используется для восстановления значения MTU по умолчанию.

Форма **show** этой команды используется для просмотра настройки MTU интерфейса агрегированных каналов Ethernet.

10.6.10 interfaces bonding <bondx> primary <ethx>

Установка одного из каналов Ethernet в составе интерфейса агрегированных каналов Ethernet в качестве основного.

Синтаксис

```
set interfaces bonding <bondx> primary <ethx>

delete interfaces bonding <bondx> primary

show interfaces bonding <bondx> primary
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   bonding bondx {
      primary ethx
   }
}
```

Параметры

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от bond0 до bond99.

ethx

Идентификатор основного интерфейса Ethernet в интерфейсе агрегированных каналов Ethernet.

Значение по умолчанию

Главный канал отсутствует.

Указания по использованию

Эта команда используется для указания основного интерфейса Ethernet в интерфейсе агрегирования каналов Ethernet.

Этот параметр необходим, если используется режим агрегирования "активный-резервный" (active-backup).

Если используется режим агрегирования "активный-резервный" и интерфейс помечен как основной, то он всегда остается единственным активным членом интерфейса агрегированных каналов Ethernet до тех пор, пока он доступен. Альтернативные интерфейсы используются только тогда, когда основной выходит из оперативного режима.

Такой вариант полезен, когда один из интерфейсов, входящих в состав интерфейса агрегированных каналов Ethernet, следует предпочесть другому, например, когда у него более высокая пропускная способность, чем у другого.

Форма **set** этой команды используется для назначения интерфейса Ethernet первичным интерфейсом в агрегировании каналов Ethernet в режиме "активный-резервный".

Форма **delete** этой команды используется для удаления у интерфейса Ethernet роли первичного интерфейса для агрегирования каналов Ethernet.

Форма **show** этой команды используется для просмотра настройки агрегирования каналов Ethernet.

10.6.11 interfaces ethernet <ethx> bond-group <bondx>

Добавление интерфейса Ethernet в состав интерфейса агрегированных каналов Ethernet.

Синтаксис

```
set interfaces ethernet <ethx> bond-group <bondx>

delete interfaces ethernet <ethx> bond-group <bondx>

show interfaces ethernet <ethx> bond-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      bond-group bondx
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

bondx

Множественный узел. Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от bond0 до bond99.

Значение по умолчанию

Отсутствуют.

Указания по использованию

Эта команда используется для добавления интерфейса Ethernet в состав интерфейса агрегированных каналов Ethernet.

Интерфейс Ethernet может входить в состав только одного интерфейса агрегированных каналов Ethernet. Интерфейс агрегированных каналов Ethernet должна быть предварительно определен с помощью команды **interfaces bonding <bondx>**. Максимальное число интерфейсов Ethernet, которое можно добавить в группу агрегирования, зависит от имеющихся системных ресурсов. Для большинства реализаций оно практически не ограничено.

ПРИМЕЧАНИЕ Если интерфейс Ethernet отключен, он не будет добавлен в группу агрегирования.

Если интерфейс Ethernet предполагается добавить в группу агрегирования, настраивать IP-адрес для него нельзя. Вместо этого настраивается IP-адрес для группы с помощью команды **interfaces bonding <bondx> address**.

Форма **set** этой команды используется для добавления интерфейса Ethernet в группу агрегирования каналов Ethernet.

Форма **delete** этой команды используется для удаления интерфейса Ethernet из группы агрегирования каналов Ethernet.

Форма **show** этой команды используется для просмотра настройки группы агрегирования.

10.6.12 show interfaces bonding

Вывод сведений о группе агрегирования интерфейсов Ethernet.

Синтаксис

```
show interfaces bonding [<bondx> | detail | slaves]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

bondx

Отображение подробных сведений об указанном интерфейсе агрегирования каналов Ethernet.

detail

Отображение подробных сведений обо всех интерфейсах агрегирования каналов Ethernet.

slaves

Отображение сведений о составляющих интерфейсах агрегирования.

Значение по умолчанию

Отображаются сведения обо всех группах агрегирования интерфейсов Ethernet.

Указания по использованию

Эта команда используется для просмотра состояния работоспособности настроенных групп агрегирования интерфейсов Ethernet.

Примеры

В примере ниже приведен вывод для команды show interfaces bonding.

Пример 104– Отображение сведений об интерфейсах агрегирования каналов Ethernet

```
admin@edge:~$ show interfaces bonding
Interface    IP Address         State       Link   Description
bond0        -                  up          up
bond1        -                  down        down
admin@edge:~$
```

В примере ниже приведен вывод команды show interfaces bonding slaves.

Пример 105– Отображение сведений об интерфейсах, входящих в состав интерфейса агрегирования каналов Ethernet

```
admin@edge:~$ show  interfaces bonding slaves
Interface    Mode                   State    Link   Slaves
bond0        802.3ad                up       up     eth1
bond1        802.3ad                down     down
admin@edge:~$
```

10.7 Интерфейсы псевдо-Ethernet

В данном разделе описано, как создать интерфейс псевдо-Ethernet, назначив несколько MAC-адресов одному физическому интерфейсу.

В данном разделе рассматриваются следующие вопросы:

- Обзор интерфейсов псевдо-Ethernet

- Команды для интерфейсов псевдо-Ethernet

Обзор интерфейсов псевдо-Ethernet

Под интерфейсом псевдо-Ethernet подразумевается создание нескольких виртуальных устройств Ethernet с различными MAC-адресами на одном физическом порту Ethernet. Интерфейсы псевдо-Ethernet используются в среде виртуализации, где они могут быть быть использованы другими виртуальными машинами. Использование интерфейсов псевдо-Ethernet требует меньше накладных расходов по сравнению с использованием сетевых мостов. Использование интерфейсов псевдо-Ethernet позволяет обойти ограничение, позволяющее создавать максимум 4096 виртуальных локальных сетей (VLANs) на одном порту Ethernet.

Виртуальные интерфейсы Ethernet ведут себя аналогично реальным устройствам Ethernet. Для них можно указать IP-адрес и сетевые настройки, описания и MAC-адреса, для того чтобы связать их с физическим портом Ethernet используется команда **interfaces pseudo-ethernet <pethx> link <ethx>**. Виртуальное устройство наследует характеристики (скорость, дуплексный режим и т.д.) физического интерфейса, с которым связан.

После определения интерфейса псевдо-Ethernet на него можно ссылаться так же как на реальный интерфейс Ethernet в правилах межсетевого экрана, политиках QoS.

При использовании интерфейсов псевдо-Ethernet необходимо учитывать следующее:

- нельзя подключиться к внутреннему интерфейсу псевдо-Ethernet из системы, в которой он определен. Например, при отправке запросов echo-request на интерфейс псевдо-Ethernet из системы в которой он определен, ответов echo-reply получено не будет;
- пакеты Ethernet не перенаправляются между интерфейсами псевдо-Ethernet;
- интерфейсы псевдо-Ethernet не поддерживают виртуальные сети (VLAN), а также нельзя включить интерфейс псевдо-Ethernet в виртуальную сеть VLAN;
- интерфейсы псевдо-Ethernet не могут быть частью интерфейса агрегированных каналов Ethernet;
- интерфейсы псевдо-Ethernet могут не работать в окружении, которое предполагает наличие только одного адреса у сетевой карты (NIC); например:
    - сетевые коммутаторы, допускающие использование единственного адреса;
    - модемы ADSL, которые «запоминают» MAC-адрес сетевой карты.

Примеры настройки интерфейса псевдо-Ethernet

На рисунке приведен простой пример использования интерфейса псевдо-Ethernet. В этом примере:

- интерфейсу Ethernet **eth1** назначен IP-адрес 192.168.10.254/24, а также он имеет MAC-адрес 0c:c2:de:45:d3:01;
- интерфейс псевдо-Ethernet **peth0** связан с физическим интерфейсом **eth1**. Для него назначен IP-адрес 192.168.100.254/24, а также MAC-адрес 02:07:b4:61:62:1a.

Следует отметить, что интерфейсу псевдо-Ethernet можно назначить сетевой префикс отличный от префикса физического интерфейса. Например, в этом примере можно назначить интерфейсу псевдо-Ethernet адрес 192.168.100.254/32.

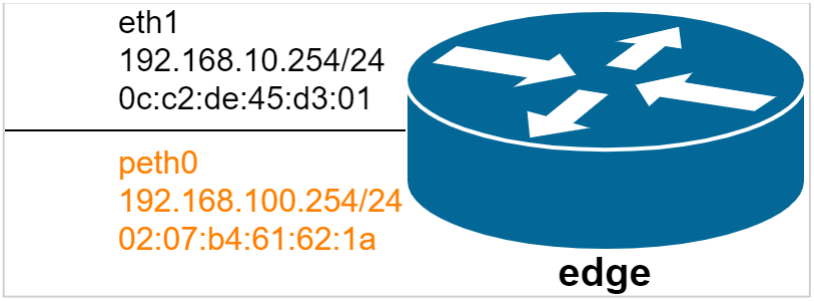


Рисунок 9 – Создание интерфейса псевдо-Ethernet

Для настройки данной схемы нужно выполнить следующие действия в режиме настройки.

Пример 106– Создание интерфейса псевдо-Ethernet

Действие	**Команда**
Создание интерфейса псевдо-Ethernet и	`[edit]`

назначение ему адреса	admin@edge# set interfaces pseudo-ethernet peth0 address 192.168.100.254/24
Привязка интерфейса псевдо-Ethernet к физическому порту Ethernet	[edit] admin@edge# set interfaces pseudo-ethernet peth0 link eth1
Назначение MAC-адреса для интерфейса псевдо-Ethernet	[edit] admin@edge# set interfaces pseudo-ethernet peth0 mac 02:07:b4:61:62:1a
Фиксация изменений	[edit] admin@edge# commit
Вывод настройки интерфейса псевдо-Ethernet	[edit] admin@edge1# show interfaces pseudo-ethernet peth0 address 192.168.100.254/24 link eth1

Команды для интерфейсов псевдо-Ethernet

Команды настройки	
interfaces pseudo-ethernet <pethx>	Определение интерфейса псевдо-Ethernet.
interfaces pseudo-ethernet <pethx> address	Назначение IP-адреса и сетевого префикса для интерфейса псевдо-Ethernet.
interfaces pseudo-ethernet <pethx> description <описание>	Создание текстового описания для интерфейса псевдо-Ethernet.
interfaces pseudo-ethernet <pethx> disable	Отключение интерфейса псевдо-Ethernet с сохранением настроек
interfaces pseudo-ethernet <pethx> link <ethx>	Определение физического интерфейса Ethernet, связанного с интерфейсом псевдо-Ethernet.
interfaces pseudo-ethernet <pethx> mac <mac-адрес>	Назначение MAC-адреса интерфейсу псевдо-Ethernet.

10.7.1 interfaces pseudo-ethernet <pethx>

Определение интерфейса псевдо-Ethernet.

Синтаксис

```
set interfaces pseudo-ethernet <pethx>

delete interfaces pseudo-ethernet <pethx>

show interfaces pseudo-ethernet <pethx>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    pseudo-ethernet pethx
}
```

Параметры

pethx

Множественный узел. Идентификатор определяемого интерфейса псевдо-Ethernet. Поддерживаются значения в диапазоне от peth0 до peth999. Можно определить несколько псевдо-интерфейсов, создав соответствующее количество узлов конфигурации **pseudo-ethernet**.

Значение по умолчанию

Отсутствуют.

Указания по использованию

Данная команда позволяет определить виртуальное устройство Ethernet (интерфейс псевдо-Ethernet), связав несколько MAC-адресов с одним физическим интерфейсом Ethernet.

Номер в идентификаторе псевдо-интерфейса никак не связан с номером в идентификаторе физического интерфейса; например, интерфейс *peth0* необязательно должен быть связан с интерфейсом *eth0*.

ПРИМЕЧАНИЕ Интерфейс псевдо-Ethernet обязательно должен быть связан с одним из физических интерфейсов Ethernet с использованием команды **interfaces pseudo-ethernet <pethx> link <ethx>**. Предварительно используемый физический интерфейс Ethernet должен быть определен в системе.

После определения интерфейса псевдо-Ethernet, ему можно назначить MAC-адрес при помощи команды **interfaces pseudo-ethernet <pethx> mac <mac-addr>** аналогично тому, как это делается для физического порта Ethernet.

Форма **set** используется для создания интерфейса псевдо-Ethernet.

Форма **delete** данной команды используется для удаления интерфейса псевдо-Ethernet.

Форма **show** данной команды используется для отображения настройки интерфейса псевдо-Ethernet.

10.7.2 interfaces pseudo-ethernet <pethx> address

Назначение IP-адреса и префикса сети для интерфейса псевдо-Ethernet.

Синтаксис

```
set interfaces ethernet <pethx> address [<ip-адрес> | dhcp]

delete interfaces ethernet <pethx> address [<ip-адрес> | dhcp]

show interfaces ethernet <pethx> address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   pseudo-ethernet pethx {
      address ip-адрес | dhcp
   }
}
```

Параметры

pethx

Множественный узел. Идентификатор определяемого интерфейса псевдо-Ethernet. Поддерживаются значения в диапазоне от peth0 до peth999.

ip-адрес

IPv4-адрес или IPv6-адрес для данного интерфейса псевдо-Ethernet. Допустимые значения представлены в таблице ниже:

Таблица 49 – Формат указания ip-адреса для интерфейса

Значение	Описание
<x.x.x.x/x>	IPv4-адрес/префикс (например: 192.168.10.254/24).
<h:h:h:h:h:h:h:h/x>	IPv6-адрес/префикс (например, 2001:db8:1234::/48)

Назначить интерфейсу несколько IP-адресов можно, создав соответствующее количество узлов конфигурации **address.**

dhcp

Параметр определяет интерфейс псевдо-Ethernet как клиент протокола DHCP, получающий адрес и префикс от сервера DHCP.

Значение по умолчанию

Отсутствуют.

Указания по использованию

Данная команда используется для назначения IP-адреса и префикса сети интерфейсу псевдо-Ethernet.

Форма **set** данной команды используется для назначения IP-адреса и префикса сети.

Форма **delete** данной команды используется для удаления настройки IP-адреса.

Форма **show** данной команды используется для отображения настройки IP-адреса.

10.7.3 interfaces pseudo-ethernet <pethx> description <описание>

Создание текстового описания для интерфейса псевдо-Ethernet.

Синтаксис

```
set interfaces ethernet <pethx> description <описание>
delete interfaces ethernet <pethx> description
show interfaces ethernet <pethx> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   pseudo-ethernet pethx {
      description описание
   }
}
```

Параметры

pethx

Множественный узел. Идентификатор определяемого интерфейса псевдо-Ethernet. Поддерживаются значения в диапазоне от peth0 до peth999.

описание

Мнемоническое имя или описание интерфейса псевдо-Ethernet.

Значение по умолчанию

Отсутствуют.

Указания по использованию

Данная команда позволяет установить текстовое описание для интерфейса псевдо-Ethernet.

Форма **set** данной команды используется для установки описания.

Форма **delete** данной команды используется для удаления описания.

Форма **show** данной команды используется для отображения настройки описания.

10.7.4 interfaces pseudo-ethernet <pethx> disable

Отключение интерфейса псевдо-Ethernet с сохранением текущей настройки.

Синтаксис

```
set interfaces pseudo-ethernet <pethx> disable
delete interfaces pseudo-ethernet <pethx> disable
show interfaces pseudo-ethernet <pethx>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   pseudo-ethernet pethx {
      disable
   }
}
```

Параметры

pethx

Множественный узел. Идентификатор определяемого интерфейса псевдо-Ethernet. Поддерживаются значения в диапазоне от peth0 до peth999.

Значение по умолчанию

Отсутствуют.

Указания по использованию

Данная команда позволяет отключить интерфейс псевдо-Ethernet без удаления настроек.

Форма **set** данной команды используется для отключения интерфейса.

Форма **delete** данной команды используется для включения интерфейса.

Форма **show** данной команды используется для отображения настройки интерфейса псевдо-Ethernet.

10.7.5 interfaces pseudo-ethernet <pethx> link <ethx>

Определение физического интерфейса Ethernet, связанного с интерфейсом псевдо-Ethernet.

Синтаксис

```
set interfaces ethernet <pethx> link <ethx>
delete interfaces ethernet <pethx> link
show interfaces ethernet <pethx> link
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   pseudo-ethernet pethx {
      link ethx
   }
}
```

Параметры

pethx

Множественный узел. Идентификатор определяемого интерфейса псевдо-Ethernet. Поддерживаются значения в диапазоне от peth0 до peth999.

ethx

Обязательный. Физический интерфейс Ethernet, связанный с интерфейсом псевдо-Ethernet. Значение должно лежать в диапазоне от eth0 до eth999 в зависимости от реально имеющихся в системе интерфейсов Ethernet. Числовые значения в идентификаторах виртуального и реального интерфейсов pethx и ethx могут не совпадать (например, интерфейс peth4 может быть связан с интерфейсом eth1).

Значение по умолчанию

Отсутствуют.

Указания по использованию

Данная команда позволяет указать физический интерфейс Ethernet, с которым связан интерфейс псевдо-Ethernet.

Форма **set** данной команды используется для указания интерфейса Ethernet.

Форма **delete** используется для удаления настройки. Следует учитывать, что указание физического интерфейса является обязательным.

Форма **show** данной команды используется для отображения настройки физического интерфейса Ethernet, связанного с данным интерфейсом псевдо-Ethernet.

10.7.6 interfaces pseudo-ethernet <pethx> mac <mac-адрес>

Указание MAC-адреса для интерфейса псевдо-Ethernet.

Синтаксис

```
set interfaces ethernet <pethx> mac <mac-адрес>

delete interfaces ethernet <pethx> mac

show interfaces ethernet <pethx> mac
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   pseudo-ethernet pethx {
      mac mac-адрес
    }
}
```

Параметры

pethx

Множественный узел. Идентификатор определяемого интерфейса псевдо-Ethernet. Поддерживаются значения в диапазоне от peth0 до peth999.

mac-адрес

MAC-адрес, который будет назначен интерфейсу псевдо-Ethernet. Адрес указывается в формате шести разделенных двоеточиями 8-битных шестнадцатеричных чисел, например, 00:0a:59:9a:f2:ba.

Значение по умолчанию

В том случае если MAC-адрес не будет указан явно, он будет назначен автоматически.

Указания по использованию

Эта команда позволяет установить MAC-адрес для интерфейса псевдо-Ethernet.

Форма **set** данной команды позволяет установить MAC-адрес для интерфейса псевдо-Ethernet.

Форма **delete** данной команды используется для удаления настройки MAC-адреса.

Форма **show** данной команды используется для отображения настройки MAC-адреса для интерфейса псевдо-Ethernet.

10.8 PPPoE

В данном разделе приведены команды для настройки подключений PPPoE.

Команды настройки	
interfaces ethernet <ethx> pppoe <номер>	Включение или отключение модуля PPPoE на указанном интерфейсе Ethernet.
interfaces ethernet <ethx> pppoe <номер>	Данная команда позволяет указать имя сервера доступа для

access-concentrator <имя>	подключения.
interfaces ethernet <ethx> pppoe <номер> compression <режим>	Данная команда позволяет указать настройки сжатия трафика.
interfaces ethernet <ethx> pppoe <номер> connection-type <тип>	Порядок установления соединения с PPPoE сервером.
interfaces ethernet <ethx> pppoe <номер> default-route <режим>	Включение или отключение автоматического добавления маршрута по умолчанию при установлении соединения PPPoE.
interfaces ethernet <ethx> pppoe <номер> idle-timeout <время>	Указание интервала времени в секундах, по истечении которого будет отключено соединение PPPoE при отсутствии передаваемого по нему сетевого трафика.
interfaces ethernet <ethx> pppoe <номер> local-address <ipv4-адрес>	Указание IP-адреса локального оконечного узла подключения PPPoE.
interfaces ethernet <ethx> pppoe <номер> mtu <mtu>	Указание MTU для интерфейса Ethernet PPPoE.
interfaces ethernet <ethx> pppoe <номер> name-server <режим>	Данная команда позволяет указать требуется ли получение адресов серверов DNS от удаленного узла соединения PPPoE.
interfaces ethernet <ethx> pppoe <номер> password <пароль>	Указание пароля, который будет использован для аутентификации на удаленном узле подключения PPPoE.
interfaces ethernet <ethx> pppoe <номер> remote-address <ipv4-адрес>	Указание IP-адреса удаленного узла подключения PPPoE.
interfaces ethernet <ethx> pppoe <номер> service-name <имя>	Позволяет выбрать сервер доступа на основе названия предоставляемого сервиса.
interfaces ethernet <ethx> pppoe <номер> user-id <идентификатор_пользователя>	Указание идентификатора пользователя, который используется при аутентификации на удаленном сервере доступа.
Эксплуатационный режим	
show interfaces pppoe	Вывод сведений и статистических данных для интерфейсов PPPoE.

10.8.1 interfaces ethernet <ethx> pppoe <номер>

Включение или отключение модуля PPPoE на указанном интерфейсе Ethernet.

Синтаксис

```
set interfaces <ethx> pppoe <номер>
delete interfaces <ethx> pppoe <номер>
show interfaces <ethx> pppoe <номер>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      pppoe номер {
      }
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

номер

Обязательный. Номер устройства PPPoE. Этот номер должен быть уникален. Интерфейс PPPoE будет иметь имя pppoeX, где X — номер устройства PPPoE (например, pppoe7). Значение должно лежать в диапазоне от 0 до 15.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет настроить устройство PPPoE (Point-to-Point over Ethernet) для указанного интерфейса Ethernet. Устройство PPPoE начинает существовать в системе только после установления сеанса PPPoE. То есть интерфейс PPPoE может быть определен, но при этом не «присутствовать» в системе.

Форма **set** данной команды позволяет определить устройство PPPoE для интерфейса Ethernet.

Форма **delete** данной команды позволяет удалить устройство PPPoE на интерфейсе Ethernet.

Форма **show** данной команды используется для отображения настройки устройства PPPoE.

10.8.2 interfaces ethernet <ethx> pppoe <номер> access-concentrator <имя>

Данная команда позволяет указать имя сервера доступа для подключения.

Синтаксис

```
set interfaces ethernet <ethx> pppoe <номер> access-concentrator <имя>
delete interfaces ethernet <ethx> pppoe <номер> access-concentrator
show interfaces ethernet <ethx> pppoe <номер> access-concentrator
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      pppoe номер {
         access-concentrator имя
      }
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

номер

Обязательный. Номер устройства PPPoE. Значение должно лежать в диапазоне от 0 до 15.

имя

Имя сервера доступа, к которому будет подключаться данное устройство PPPoE.

Значение по умолчанию

Отсутствует.

Указания по использованию

При использовании данной команды устройство PPPoE будет инициировать сеанс только с указанным сервером доступа.

Установление подключения PPPoE начинается с фазы обнаружения сервера доступа (discovery stage). Для инициализации сеанса PPPoE клиент посылает на широковещательный адрес специальный пакет PADI (PPPoE Active Discovery Initiation). Сервер доступа отвечает пакетом PADO (PPPoE Active Discovery Offer), в который

включает свое название (Access Concentrator Name) и название предоставляемого сервиса (Service Name). Данный пакет содержит MAC-адрес конкретного сервера. Далее клиент выбирает требуемый сервер доступа и сервис из возможно нескольких предложений (пакетов PADO) и отвечает уже конкретному серверу пакетом PADR (Active Discovery Request).

Использование данной команды определяет какому серверу доступа будет направлен пакет PADR. Данную команду следует использовать в том случае, если необходимо указать конкретный сервер при наличии нескольких серверов доступа в сети.

Форма **set** данной команды позволяет указать имя сервера доступа.

Форма **delete** данной команды используется для удаления настройки сервера доступа.

Форма **show** данной команды используется для отображения конфигурации сервера доступа в сети.

10.8.3 interfaces ethernet <ethx> pppoe <номер> compression <режим>

Данная команда позволяет указать настройки сжатия трафика.

Синтаксис

```
set interfaces ethernet <ethx> pppoe <номер> compression <режим>
delete interfaces ethernet <ethx> pppoe <номер> compression
show interfaces ethernet <ethx> pppoe <номер> compression
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      pppoe номер {
         compression режим
      }
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

номер

Обязательный. Номер устройства PPPoE. Значение должно лежать в диапазоне от 0 до 15.

режим

Указывает использование сжатия трафика. Допустимые значения представлены ниже:

none: Не использовать сжатие трафика;

mppe: Использовать протокол шифрования трафика MPPE.

Значение по умолчанию

Отсутствует.

Указания по использованию

Использование данной команды определяет настройки сжатия для PPPoE соединения.

Форма **set** данной команды позволяет указать имя сервера доступа.

Форма **delete** данной команды используется для удаления настройки сервера доступа.

Форма **show** данной команды используется для отображения конфигурации сервера доступа в сети.

10.8.4 interfaces ethernet <ethx> pppoe <номер> connection-type <тип>

Порядок установления соединения с сервером.

Синтаксис

```
set interfaces ethernet <ethx> pppoe <номер> connection-type <тип>
delete interfaces ethernet <ethx> pppoe <номер> connection-type
show interfaces ethernet <ethx> pppoe <номер> connection-type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      pppoe номер {
         connection-type тип
      }
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

номер

Обязательный. Номер устройства PPPoE. Значение должно лежать в диапазоне от 0 до 15.

тип

Обязательный. Порядок установления соединения с PPPoE сервером. Допустимые значения:

on-demand: Установка соединения по требованию(при появлении трафика, интерфейс виден всегда)

persist: Установка непрерывного соединения.

Значение по умолчанию

По умолчанию с PPPoE сервером устанавливается непрерывное соединение (значение **persist**).

Указания по использованию

Если установлено значение **persist**, PPPoE соединение устанавливается после применения конфигурации. Когда соединение по какой-либо причине разрывается, сразу же производятся попытки автоматического восстановления соединения.

При установлении значения **on-demand** – PPPoE соединение будет устанавливаться только тогда, через него потребуется передать трафик. В период простоя (отсутствия трафика) соединение разрывается по истечении интервала, установленного параметром **idle-timeout**. В том случае если в период простоя соединение разрывается, оно будет установлено только тогда, когда потребуется заново передать трафик через это соединение. Интерфейс *pppoe* даже при разрыве соединения всегда находится в состоянии *up*.

При использовании данной команды также необходимо указать удаленный адрес, для этого используется команда **interfaces ethernet <ethx> pppoe <номер> remote-address <ipv4-адрес>**.

Форма **set** данной команды используется для установления подключения по запросу.

Форма **delete** данной команды используется для удаления конфигурации и восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения конфигурации.

10.8.5 interfaces ethernet <ethx> pppoe <номер> default-route <режим>

Включение или отключение автоматического добавления маршрута по умолчанию при установлении соединения PPPoE.

Синтаксис

```
set interfaces ethernet <ethx> pppoe <номер> default-route <режим>
delete interfaces ethernet <ethx> pppoe <номер> default-route
show interfaces ethernet <ethx> pppoe <номер> default-route
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      pppoe номер {
         default-route режим
      }
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

номер

Обязательный. Номер устройства PPPoE. Значение должно лежать в диапазоне от 0 до 15.

режим

Обязательный. Определяет включено ли автоматическое добавление маршрута по умолчанию при установлении соединения PPPoE. Допустимые значения:

auto*:* Процесс PPP автоматически добавит маршрут по умолчанию к удаленному узлу соединения;

none*:* Маршрут по умолчанию не добавляется.

Значение по умолчанию

При установлении соединения PPPoE автоматически добавляется маршрут по умолчанию к удаленному узлу соединения (установлено значение **auto**).

Указания по использованию

Данная команда позволяет определить, будет ли добавляться маршрут по умолчанию при установлении соединения PPPoE.

Маршрут по умолчанию будет добавлен только в том случае, если в системе до этого не было настроено другого маршрута по умолчанию.

Форма **set** данной команды позволяет включить или отключить добавление маршрута по умолчанию при установлении соединения PPPoE.

Форма **delete** данной команды используется для удаления конфигурации и восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения конфигурации.

10.8.6 interfaces ethernet <ethx> pppoe <номер> idle-timeout <время>

Указание интервала времени в секундах, по истечении которого будет отключено соединение PPPoE при отсутствии передаваемого по нему сетевого трафика.

Синтаксис

```
set interfaces ethernet <ethx> pppoe <номер> idle-timeout <таймаут>
delete interfaces ethernet <ethx> pppoe <номер> idle-timeout
show interfaces ethernet <ethx> pppoe <номер> idle-timeout
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      pppoe номер {
         idle-timeout время
      }
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

номер

Обязательный. Номер устройства PPPoE. Значение должно лежать в диапазоне от 0 до 15.

время

Интервал времени в секундах. Если установлено подключение по запросу и в течении данного интервала времени через соединение PPPoE не передается сетевой трафик, соединение отключается. Значение должно лежать в диапазоне от 0 до 4294967295, если установлено значение 0 — простаивающие соединения не отключаются.

Значение по умолчанию

По умолчанию простаивающие подключения не отключаются (установлено значение 0).

Указания по использованию

Данная команда используется для установки таймаута для подключений PPPoE по запросу.

Если используется подключение по запросу, соединение PPPoE устанавливается только тогда, когда необходимо передать трафик через это соединение. В том случае если соединение по какой-либо причине разрывается, оно устанавливается заново только тогда, когда необходимо передать трафик.

При использовании подключения по запросу необходимо также указать период простоя, по истечении которого соединение PPPoE будет отключено. В том случае если ненулевой период простоя не настроен и используется подключение по запросу, соединение, после того как оно будет установлено, не будет отключено при отсутствии сетевого трафика.

Подключение по запросу настраивается при помощи команды interfaces ethernet <ethx> pppoe <номер> connect-on-demand.

Форма **set** данной команды позволяет указать таймаут для подключения по запросу.

Форма **delete** данной команды используется для удаления конфигурации и восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения конфигурации.

10.8.7 interfaces ethernet <ethx> pppoe <номер> local-address <ipv4-адрес>

Указание IP-адреса локального оконечного узла подключения PPPoE.

Синтаксис

```
set interfaces ethernet <ethx> pppoe <номер> local-address <ipv4-адрес>
delete interfaces ethernet <ethx> pppoe <номер> local-address
show interfaces ethernet <ethx> pppoe <номер> local-address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      pppoe номер {
         local-address ipv4-адрес
      }
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

номер

Обязательный. Номер устройства PPPoE. Значение должно лежать в диапазоне от 0 до 15.

ipv4-адрес

IPv4-адрес локальной оконечной точки подключения PPPoE. Может быть указан только один локальный адрес.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для установки IP-адреса локального оконечного узла подключения PPPoE. В том случае если значение для данного параметра явно не указано, оно будет автоматически согласовано.

Форма **set** данной команды позволяет указать IP-адрес.

Форма **delete** данной команды используется для удаления конфигурации IP-адреса.

Форма **show** данной команды используется для отображения конфигурации.

10.8.8 interfaces ethernet <ethx> pppoe <номер> mtu <mtu>

Указание MTU для интерфейса Ethernet PPPoE.

Синтаксис

```
set interfaces ethernet <ethx> pppoe <номер> mtu <mtu>
delete interfaces ethernet <ethx> pppoe <номер> mtu
show interfaces ethernet <ethx> pppoe <номер> mtu
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
```

```
    ethernet ethx {
        pppoe номер {
            mtu mtu
        }
    }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

номер

Обязательный. Номер устройства PPPoE. Значение должно лежать в диапазоне от 0 до 15.

mtu

Значение MTU для интерфейса PPPoE. Пакеты, размер которых превышает установленное значение, будут фрагментированы. Значение должно лежать в диапазоне от 68 до 1492.

Значение по умолчанию

В том случае если значение для данного параметра явно не указано, значение MTU для интерфейса PPPoE будет равно значению MTU, установленному для интерфейса Ethernet минус 8 байт.

Указания по использованию

Данная команда используется для установки значения MTU (Maximum Transfer Unit) для интерфейса PPPoE. Пакеты, размер которых превышает установленное значение, будут фрагментированы.

Форма **set** данной команды позволяет установить значение MTU.

Форма **delete** данной команды используется для удаления конфигурации и восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения конфигурации.

10.8.9 interfaces ethernet <ethx> pppoe <номер> name-server <режим>

Данная команда позволяет указать требуется ли получение адресов серверов DNS от удаленного узла соединения PPPoE.

Синтаксис

```
set interfaces ethernet <ethx> pppoe <номер> name-server <режим>
delete interfaces ethernet <ethx> pppoe <номер> name-server
show interfaces ethernet <ethx> pppoe <номер> name-server
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    ethernet ethx {
        pppoe номер {
            name-server режим
        }
    }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

номер

Обязательный. Номер устройства PPPoE. Значение должно лежать в диапазоне от 0 до 15.

режим

Обязательный. Значение для данного параметра определяет требуется ли получать параметры серверов DNS от удаленного узла. Поддерживаемые значения:

auto: Локальный узел получает параметры серверов DNS от удаленного узла;

none: Локальный узел использует параметры DNS, установленные локально.

Значение по умолчанию

По умолчанию локальный узел получает параметры серверов DNS от удаленного узла.

Указания по использованию

Данная команда позволяет указать, какие настройки серверов DNS будут использоваться при установлении подключения PPPoE. Если установлено значение **auto**, используются параметры, полученные от удаленного узла. Если установлено значение **none**, используются параметры настроенные локально для данной системы.

Форма **set** данной команды позволяет указать, следует ли получать настройки серверов DNS от удаленного узла.

Форма **delete** данной команды используется для удаления текущей конфигурации и восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения текущей конфигурации.

10.8.10 interfaces ethernet <ethx> pppoe <номер> password <пароль>

Указание пароля, который будет использован для аутентификации на удаленном узле подключения PPPoE.

Синтаксис

```
set interfaces ethernet <ethx> pppoe <номер> password <пароль>

delete interfaces ethernet <ethx> pppoe <номер> password

show interfaces ethernet <ethx> pppoe <номер> password
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      ppoe номер {
         password пароль
      }
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

номер

Обязательный. Номер устройства PPPoE. Значение должно лежать в диапазоне от 0 до 15.

пароль

Обязательный. Пароль, используемый для аутентификации локального узла на удаленном сервере PPPoE.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания пароля, используемого для аутентификации локального узла на удаленном сервере PPPoE. Аутентификация не является обязательной с системной точки зрения, но большинство провайдеров требуют ее использования.

Пароль используется в сочетании с идентификатором пользователя, который указывается при помощи команды **interfaces ethernet <ethx> pppoe <номер> user-id <идентификатор_пользователя>**. Протокол аутентификации определяется удаленным узлом.

Форма **set** данной команды позволяет указать пароль.

Форма **delete** данной команды используется для удаления конфигурации пароля.

Форма **show** данной команды используется для отображения конфигурации.

10.8.11 interfaces ethernet <ethx> pppoe <номер> remote-address <ipv4-адрес>

Указание IP-адреса удаленного узла подключения PPPoE.

Синтаксис

```
set interfaces ethernet <ethx> pppoe <номер> remote-address <ipv4-адрес>

delete interfaces ethernet <ethx> pppoe <номер> remote-address

show interfaces ethernet <ethx> pppoe номер remote-address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      pppoe номер {
         remote-address ipv4-адрес
      }
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

номер

Обязательный. Номер устройства PPPoE. Значение должно лежать в диапазоне от 0 до 15.

ipv4-адрес

IP-адрес удаленного оконечного узла подключения PPPoE. Может быть указан только один удаленный адрес.

Значение по умолчанию

Отсутствует

Указания по использованию

Данная команда используется для указания IP-адреса удаленного оконечного узла подключения PPPoE. В том случае если значение для данного параметра явно не указано, адрес будет автоматически согласован.

Форма **set** данной команды позволяет указать удаленный IP-адрес.

Форма **delete** данной команды используется для удаления конфигурации.

Форма **show** данной команды используется для отображения конфигурации.

10.8.12 interfaces ethernet <ethx> pppoe <номер> service-name <имя>

Позволяет выбрать сервер доступа на основе названия предоставляемого сервиса.

Синтаксис

```
set interfaces ethernet <ethx> pppoe <номер> service-name <имя>
delete interfaces ethernet <ethx> pppoe <номер> service-name
show interfaces ethernet <ethx> pppoe <номер>  service-name
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      pppoe номер {
         service-name имя
      }
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

номер

Обязательный. Номер устройства PPPoE. Значение должно лежать в диапазоне от 0 до 15.

имя

Название сервиса. Локальный узел будет направлять запросы на подключение только тем серверам доступа, которые предоставляют указанный сервис.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать имя сервиса, на основе которого будет осуществляться выбор сервера доступа для отправки запросов на подключение.

Форма **set** данной команды позволяет указать название сервиса.

Форма **delete** данной команды используется для удаления конфигурации.

Форма **show** данной команды используется для отображения конфигурации.

10.8.13 interfaces ethernet <ethx> pppoe <номер> user-id <идентификатор_пользователя>

Указание идентификатора пользователя, который используется при аутентификации на удаленном сервере доступа.

Синтаксис

```
set interfaces ethernet <ethx> pppoe <номер> user-id
<идентификатор_пользователя>
```

```
delete interfaces ethernet <ethx> pppoe <номер> user-id
show interfaces ethernet <ethx> pppoe <номер> user-id
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   ethernet ethx {
      pppoe номер {
        user-id идентификатор_пользователя
      }
   }
}
```

Параметры

ethx

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

номер

Обязательный. Номер устройства PPPoE. Значение должно лежать в диапазоне от 0 до 15.

идентификатор_пользователя

Идентификатор пользователя, используемый для аутентификации локального узла на удаленном сервере доступа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для установки идентификатора пользователя. С системной точки зрения аутентификация не является обязательной. Однако большинство провайдеров требуют обязательного использования аутентификации.

Идентификатор пользователя используется совместно с паролем. Пароль устанавливается при помощи команды **interfaces ethernet <ethx> pppoe <номер> password <пароль>**. Протокол аутентификации определяется удаленным узлом.

Форма **set** данной команды позволяет указать идентификатор пользователя.

Форма **delete** данной команды используется для удаления конфигурации.

Форма **show** данной команды используется для отображения конфигурации.

10.8.14 show interfaces pppoe

Вывод сведений и статистических данных для интерфейсов PPPoE.

Синтаксис

```
show interfaces pppoe [<pppoex> [capture [not port <порт> | port <порт>] |
log tail | queue [class | filter]]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

pppoex

Отображение сведений для указанного интерфейса PPPoE.

capture

Перехват и отображение трафика на указанном интерфейсе PPPoE.

not port *порт*

Отображение сетевого трафика, записанного на всех портах, кроме указанного.

port *порт*

Отображение сетевого трафика, записанного на указанном порту.

log tail

Отображение сообщений протокола PPP из журнала.

queue

Отображение сведений об очередях для интерфейса PPPoE.

class

Отображение классов очередей для указанного интерфейса.

filter

Отображение фильтров очередей для указанного интерфейса.

Значение по умолчанию

Вывод сведений для всех интерфейсов

Указания по использованию

Эта команда позволяет вывести сведения обо всех настроенных интерфейсах PPPoE.

Примеры

В примере ниже выводятся сведения об интерфейсе pppoe1

Пример 107– Вывод сведений об интерфейсе pppoe1

```
admin@edge:~$ show interfaces pppoe pppoe1
pppoe1: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1492 qdisc pfifo_fast
state UNKNOWN qlen 3
link/ppp
inet 192.168.10.2 peer 192.168.255.1/32 scope global pppoe1

RX: bytes packets errors dropped overrun mcast
165 25 0 0 0 0
TX: bytes packets errors dropped carrier collisions
183 25 0 0 0 0
```

10.9 Перенаправление и зеркалирование входящего трафика на интерфейсах

В данном разделе описаны следующие команды.

Команды настройки	
interfaces <интерфейс> redirect <имя_интерфейса>	Перенаправление всего входящего трафика с указанного интерфейса на другой.
interfaces <интерфейс> mirror <имя_интерфейса>	Зеркалирование (дублирование) всего входящего трафика с указанного интерфейса на другой.

10.9.1 interfaces <интерфейс> redirect <имя_интерфейса>

Перенаправление всего входящего трафика с указанного интерфейса на другой.

Синтаксис

```
set interfaces <интерфейс> redirect <имя_интерфейса>

delete interfaces <интерфейс> redirect <имя_интерфейса>

show interfaces <интерфейс> redirect <имя_интерфейса>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   интерфейс {
      redirect имя_интерфейса
   }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже в разделе Указания по использованию.

имя_интерфейса

Обязательный. Указание интерфейса (например, eth1), на который будет перенаправляться весь входящий трафик. Интерфейс должен быть определён в системе.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для перенаправления всего входящего трафика с одного интерфейса на другой. Таким образом, весь входящий трафик на интерфейсе, с которого производится перенаправление, становится исходящим на указанном интерфейсе. При перенаправлении, на прохождение входящего трафика не распространяются правила МЭ, политики маршрутизации, модификации и клонирования трафика, а также политики QoS (кроме политик QoS, применение которых не подразумевает использование определённых фильтров трафика).

В приведенной ниже таблице показаны типы поддерживаемых интерфейсов и синтаксис.

Таблица 50 – Типы интерфейсов

Тип интерфейса	Синтаксис
Агрегирование каналов	bonding bondx
Виртуальный интерфейс агрегированных каналов	bonding bondx vif идентификатор_vlan
Сетевой мост	bridge brx
Ethernet	ethernet ethx
Ethernet PPPoE	ethernet ethx pppoe номер
Виртуальный интерфейс Ethernet	ethernet ethx vif идентификатор_vlan
Ethernet Vif PPPoE	ethernet ethx vif идентификатор_vlan pppoe номер
Интерфейс заглушки	loopback lo
Многоканальная связь	multilink mlx
OpenVPN	openvpn vtunx
Псевдо-Ethernet	pseudo-ethernet pethx
Последовательный интерфейс	serial srx vif идентификатор_vlan
Туннель	tunnel tunx

Форма **set** данной команды используется для указания интерфейсов участвующих в перенаправлении трафика.

Форма **delete** данной команды используется для отключения функции перенаправления трафика.

Форма **show** данной команды используется для отображения настройки перенаправления трафика.

10.9.2 interfaces <интерфейс> mirror <имя_интерфейса>

Зеркалирование (дублирование) всего входящего трафика с указанного интерфейса на другой.

Синтаксис

```
set interfaces <интерфейс> mirror <имя_интерфейса>
delete interfaces <интерфейс> mirror <имя_интерфейса>
show interfaces <интерфейс> mirror <имя_интерфейса>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   интерфейс {
      mirror имя_интерфейса
   }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже в разделе Указания по использованию.

имя_интерфейса

Обязательный. Указание интерфейса (например, eth1), на который будет дублироваться весь входящий трафик. Интерфейс должен быть определён в системе.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для дублирования всего входящего трафика с одного интерфейса на другой. Таким образом, весь входящий трафика на интерфейсе, с которого производится зеркалирование, дублируется на указанный интерфейс, для которого этот трафик становится исходящим. При зеркалировании, на дублированный трафик не распространяются правила МЭ, политики маршрутизации, модификации и клонирования трафика, а также политики QoS (кроме политик QoS, применение которых не подразумевает использование определённых фильтров трафика).

В приведенной ниже таблице показаны типы поддерживаемых интерфейсов и синтаксис.

Таблица 51 – Типы интерфейсов

Тип интерфейса	Синтаксис
Агрегирование каналов	bonding bondx
Виртуальный интерфейс агрегированных каналов	bonding bondx vif идентификатор_vlan
Сетевой мост	bridge brx
Ethernet	ethernet ethx
Ethernet PPPoE	ethernet ethx pppoe номер
Виртуальный интерфейс Ethernet	ethernet ethx vif идентификатор_vlan
Ethernet Vif PPPoE	ethernet ethx vif идентификатор_vlan pppoe номер
Интерфейс заглушки	loopback lo
Многоканальная связь	multilink mlx
OpenVPN	openvpn vtunx
Псевдо-Ethernet	pseudo-ethernet pethx
Последовательный интерфейс	serial srx vif идентификатор_vlan

Тип интерфейса	Синтаксис
Туннель	tunnel tunx

Форма **set** данной команды используется для указания интерфейсов участвующих в зеркалировании трафика.

Форма **delete** данной команды используется для отключения функции зеркалирования трафика.

Форма **show** данной команды используется для отображения настройки зеркалирования трафика.

11 Статистическая маршрутизация

11.1 Настройка статических маршрутов

11.1.1 Обзор статических маршрутов

Статический маршрут это маршрут, настроенный вручную, который, в общем случае, не может быть обновлен динамически по сведениям о топологии сети, которые получает Numa Edge. Однако если канал терпит сбой, маршрутизатор удалит из таблицы маршрутизации маршруты, в том числе статические, в которых этот интерфейс использовался для достижения следующего транзитного узла.

В общем случае статические маршруты следует использовать только для сетей с очень простой топологией, либо для переопределения поведения протокола динамической маршрутизации для небольшого числа маршрутов.

Все маршруты, которые маршрутизатор получает из настройки или от протоколов динамической маршрутизации, хранятся в таблице маршрутизации (RIB).

Одноадресные маршруты непосредственно используются для определения таблицы пересылки, используемой для пересылки пакетов одноадресной передачи.

11.1.2 Плавающие статические маршруты

Обычно статические маршруты имеют относительно короткое административное расстояние — обычно оно равно 1 и, как правило, оно меньше, чем административное расстояние для динамических маршрутов. Плавающим называется статический маршрут, имеющий административное расстояние большее, чем административное расстояние для динамического маршрута.

Чтобы настроить статический маршрут в качестве плавающего, следует установить для него административное расстояние больше того, которое применяется в используемом протоколе динамической маршрутизации. В этом случае статический маршрут будет менее предпочтителен, чем динамический маршрут. При этом статический маршрут выполняет роль альтернативного пути, по которому сетевой трафик будет направляться в том случае, если динамический маршрут станет недоступен.

11.1.3 Пример настройки статических маршрутов

В этом примере представлены образцы настроек для основных статических маршрутов. После выполнения всех действий система будет настроена в соответствии с рисунком ниже. В этом примере создается статический маршрут, фактически указывающий, что «все пакеты, адресованные в сеть 192.168.20.0/24, следует переслать на адрес 192.168.12.254».

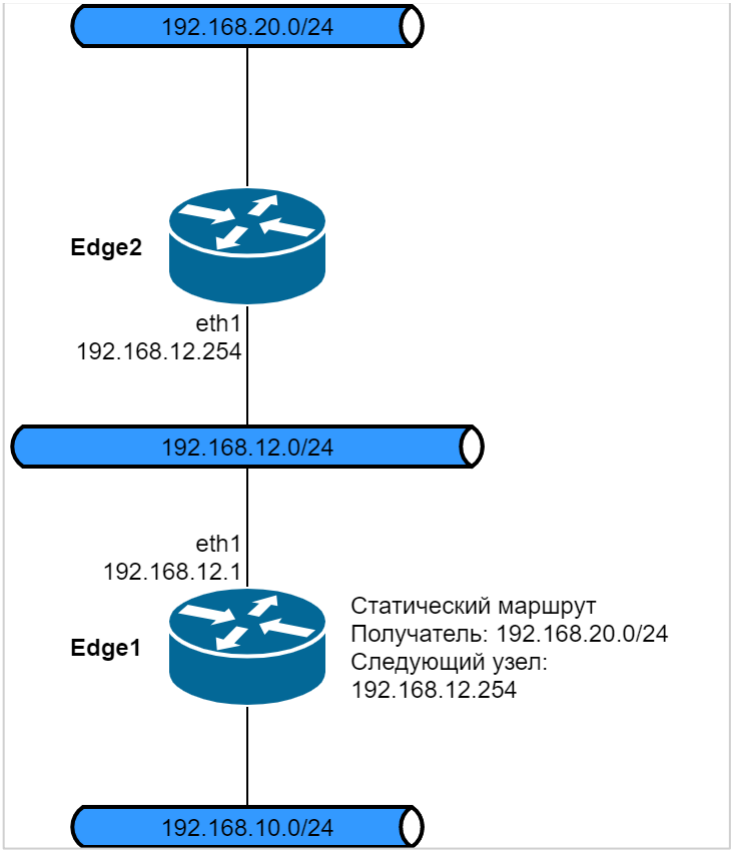


Рисунок 10 – Статические маршруты

В примере выполняется создание статического маршрута к сети 192.168.20.0/24, направляемого через узел 192.168.12.254. Для создания статического маршрута необходимо выполнить следующую последовательность команд в режиме настройки:

Пример 108– Создание статического маршрута

Действие	**Команда**
Создание статического маршрута к Edge2.	`[edit]` `admin@Edge1# set protocols static route 192.168.20.0/24 next-hop 192.168.12.254`
Фиксация настройки.	`[edit]` `admin@Edge1# commit`

11.2 Команды статической маршрутизации

В данном разделе приведены следующие команды:

Команды настройки	
Команды настройки статической маршрутизации IPv4	
protocols static arp <ipv4-адрес> hwaddr <mac-адрес>	Установка статической трансляции ARP.
protocols static interface-route <ipv4-подсеть> next-hop-interface <интерфейс>	Установка интерфейса следующего транзитного узла для статического маршрута IPv4-трафика, основанного на интерфейсе.
protocols static route <ipv4-подсеть> blackhole	Настройка статического маршрута IPv4-трафика в "черную дыру".
protocols static route <ipv4-подсеть> next-hop <ipv4-адрес>	Установка следующего транзитного узла статического маршрута.
Команды настройки статической маршрутизации IPv6	
protocols static interface-route6 <ipv6-подсеть> next-hop-interface <интерфейс>	Установка интерфейса следующего транзитного узла для статического маршрута IPv6-трафика, основанного на интерфейсе.

protocols static route6 <ipv6-подсеть> blackhole	Настройка статического маршрута IPv6-трафика в "черную дыру".
protocols static route6 <ipv6-подсеть> next-hop <ipv6-адрес>	Установка следующего транзитного узла статического маршрута IPv6-трафика.
Команды настройки таблиц маршрутизации	
protocols static table <имя_таблицы>	Определение таблицы маршрутизации.
protocols static table <имя_таблицы> dhcp <интерфейс>	Установка получения маршрутов по протоколу DHCP с указанного интерфейса.
protocols static table <имя_таблицы> interface-route <ipv4-подсеть> next-hop-interface <интерфейс>	Установка следующего транзитного узла для статического маршрута, основанного на интерфейсе.
protocols static table <имя_таблицы> route <ipv4-подсеть> blackhole	Настройка статического маршрута в таблице маршрутизации в «черную дыру».
protocols static table <имя_таблицы> route <ipv4-подсеть> next-hop <ipv4-адрес>	Установка следующего транзитного узла статического маршрута.
Эксплуатационные команды	
policy clear prefix-list	Очистка статистики или состояния для списка префиксов.
clear ip route cache	Очистка кэша маршрутизации ядра для протокола IPv4.
show ip forwarding	Отображение состояния пересылки пакетов для протокола IPv4.
show ip route	Отображение маршрутов, содержащихся в таблице маршрутизации и таблице пересылки для протокола IPv4.
show ip route cache	Отображение кэша маршрутизации ядра для протокола IPv4.
show ip route connected	Отображение маршрутов, подключенных напрямую для протокола IPv4.
show ip route forward	Отображение маршрутов, которые содержатся в таблице пересылки (Forwarding Information Base, FIB) для протокола IPv4.
show ip route kernel	Отображение маршрутов ядра для протокола IPv4.
show ip route static	Отображение статических маршрутов для протокола IPv4.
show ip route summary	Отображение кратких сведений о маршрутах для протокола IPv4.
show ip route supernets-only	Отображение маршрутов вышестоящих сетей для протокола IPv4.
clear ipv6 neighbors	Очистка кэша протокола определения соседей IPv6.
clear ipv6 route cache	Очистка кэша маршрутизации ядра для протокола IPv6.
show ipv6 forwarding	Отображение состояния пересылки пакетов для протокола IPv6.
show ipv6 neighbors	Отображение информации протокола определения соседей IPv6.
show ipv6 route	Отображение маршрутов, содержащихся в таблице маршрутизации и таблице пересылки для протокола IPv6.
show ipv6 route cache	Отображение кэша маршрутизации ядра для протокола IPv6.
show ipv6 route connected	Отображение маршрутов, подключенных напрямую для протокола IPv6.
show ipv6 route forward	Отображение маршрутов, которые содержатся в таблице пересылки (Forwarding Information Base, FIB) для протокола IPv6.
show ipv6 route kernel	Отображение маршрутов ядра для протокола IPv6.
show ipv6 route static	Отображение статических маршрутов для протокола IPv6.

show ipv6 route summary	Отображение кратких сведений о маршрутах для протокола IPv6.
routing table show	Отображение таблицы маршрутизации системы.

11.2.1 protocols static arp <ipv4-адрес> hwaddr <mac-адрес>

Установка статической трансляции ARP.

Синтаксис

```
set protocols static arp <ipv4-адрес> hwaddr <mac-адрес>
delete protocols static arp <ipv4-адрес> hwaddr <mac-адрес>
show protocols static arp
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   static {
      arp ipv4-адрес {
         hwaddr mac-адрес
      }
   }
}
```

Параметры

ipv4-адрес

IPv4-адрес для проверки соответствия.

mac-адрес

MAC-адрес для проверки соответствия. Адрес указывается в формате шести разделенных двоеточиями 8-битных шестнадцатеричных чисел, например, 00:0a:59:9a:f2:ba.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для настройки статической трансляции ARP.

Форма **set** данной команды позволяет добавить связку IPv4-адреса и MAC-адреса в таблицу ARP.

Форма **delete** данной команды позволяет удалить связку IPv4-адреса и MAC-адреса из таблицы ARP.

Форма **show** позволяет просмотреть статические записи в таблице ARP.

11.2.2 protocols static interface-route <ipv4-подсеть> next-hop-interface <интерфейс>

Установка интерфейса следующего транзитного узла для статического маршрута IPv4-трафика, основанного на интерфейсе.

Синтаксис

```
set protocols static interface-route <ipv4-подсеть> next-hop-interface <интерфейс> [disable | distance <расстояние>]
delete protocols static interface-route <ipv4-подсеть> next-hop-interface <интерфейс> [disable | distance]
show protocols static interface-route <ipv4-подсеть> next-hop-interface <интерфейс> [disable | distance]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    static {
        interface-route ipv4-подсеть {
            next-hop-interface интерфейс {
                disable            distance расстояние
            }
        }
    }
}
```

Параметры

ipv4-подсеть

Обязательный. Множественный узел. Определение статического маршрута, основанного на интерфейсе. Подсеть получателя указывается в формате IPv4-адрес/префикс. Чтобы создать несколько маршрутов, основанных на интерфейсе, следует создать соответствующее количество узлов конфигурации interface-route.

интерфейс

Обязательный. Интерфейс, на который необходимо перенаправить трафик для указанной подсети. Интерфейс должен быть заранее определен в системе.

disable

Отключение статического маршрута на основе интерфейса.

расстояние

Необязательный. Установка расстояния до следующего узла для данного маршрута. Чем меньше расстояние, назначенное маршруту, тем больший он имеет приоритет. Значение должно лежать в диапазоне от 1 до 255. Значение по умолчанию равно 1.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для настройки на маршрутизаторе статического маршрута на основе интерфейса для IPv4-трафика.

Форма **set** данной команды позволяет указать интерфейс следующего транзитного узла для данного маршрута.

Форма **delete** данной команды позволяет удалить интерфейс следующего транзитного узла.

Форма **show** позволяет просмотреть интерфейс следующего транзитного узла для данного маршрута.

11.2.3 protocols static route <ipv4-подсеть> blackhole

Настройка статического маршрута в "черную дыру" для IPv4-трафика.

Синтаксис

```
set protocols static route <ipv4-подсеть> blackhole [distance <расстояние>]
delete protocols static route <ipv4-подсеть> blackhole [distance]
show protocols static route <ipv4-подсеть> blackhole [distance]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   static {
      route ipv4-подсеть {
         blackhole {
            distance расстояние
         }
      }
   }
}
```

Параметры

ipv4-подсеть

Обязательный. Множественный узел. Определение статического маршрута. Подсеть получателя указывается в формате адрес/префикс. Чтобы определить несколько статических маршрутов, следует создать соответствующее количество узлов конфигурации route.

расстояние

Необязательный. Указание расстояния для маршрута к «черной дыре». Чем меньше расстояние, назначенное маршруту, тем больший он имеет приоритет. Значение должно лежать в диапазоне от 1 до 255. Значение по умолчанию равно 1.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для настройки маршрута к «черной дыре». Маршрут к «черной дыре» - это маршрут, все пакеты для которого отбрасываются.

Форма **set** данной команды используется для установки маршрута к «черной дыре».

Форма **delete** используется для удаления маршрута к «черной дыре».

Форма **show** данной команды используется для просмотра настройки маршрута к «черной дыре».

11.2.4 protocols static route <ipv4-подсеть> next-hop <ipv4-адрес>

Установка адреса следующего узла для статического маршрута.

Синтаксис

```
set protocols static route <ipv4-подсеть> next-hop <ipv4-адрес> [disable | distance <расстояние>]

delete protocols static route <ipv4-подсеть> next-hop <ipv4-адрес> [disable | distance]

show protocols static route <ipv4-подсеть> next-hop <ipv4-адрес> [disable | distance]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   static {
      route ipv4-подсеть {
         next-hop ipv4-адрес {
            disable
```

```
            distance расстояние
        }
    }
}
```

Параметры

ipv4-подсеть

Обязательный. Множественный узел. Определение статического маршрута. Подсеть получателя указывается в формате адрес/префикс. Чтобы определить несколько статических маршрутов, следует создать соответствующее количество узлов конфигурации route.

ipv4-адрес

Обязательный. Адрес следующего узла.

disable

Отключение статического маршрута.

расстояние

Необязательный. Установка расстояния до следующего узла для данного маршрута. Чем меньше расстояние, назначенное маршруту, тем больший он имеет приоритет. Значение должно лежать в диапазоне от 1 до 255. Значение по умолчанию равно 1.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для настройки статического маршрута.

Форма **set** данной команды позволяет указать следующий транзитный узел для данного маршрута.

Форма **delete** данной команды позволяет удалить следующий транзитный узел для статического маршрута.

Форма **show** данной команды позволяет вывести настройку следующего транзитного узла для статического маршрута.

11.2.5 protocols static interface-route6 <ipv6-подсеть> next-hop-interface <интерфейс>

Установка интерфейса следующего узла для статического маршрута IPv6-трафика, основанного на интерфейсе.

Синтаксис

```
set protocols static interface-route6 <ipv6-подсеть> next-hop-interface <интерфейс> [disable | distance <расстояние>]

delete protocols static interface-route6 <ipv6-подсеть> next-hop-interface <интерфейс> [disable | distance]

show protocols static interface-route6 <ipv6-подсеть> next-hop-interface <интерфейс> [disable | distance]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    static {
        interface-route6 ipv6-подсеть {
            next-hop-interface интерфейс {
```

```
            disable
            distance расстояние
        }
    }
  }
}
```

Параметры

ipv6-подсеть

Обязательный. Множественный узел. Определение статического маршрута, основанного на интерфейсе. Подсеть получателя указывается в формате адрес/префикс. Чтобы создать несколько маршрутов, основанных на интерфейсе, следует создать соответствующее количество узлов конфигурации interface-route6.

интерфейс

Обязательный. Интерфейс, на который необходимо перенаправить трафик для указанной подсети. Интерфейс должен быть заранее определен в системе.

disable

Отключение статического маршрута на основе интерфейса.

расстояние

Необязательный. Установка расстояния до следующего узла для данного маршрута. Чем меньше расстояние, назначенное маршруту, тем больший он имеет приоритет. Значение должно лежать в диапазоне от 1 до 255. Значение по умолчанию равно 1.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для настройки на маршрутизаторе статического маршрута на основе интерфейса для IPv6-трафика.

Форма **set** данной команды позволяет указать интерфейс следующего транзитного узла для данного маршрута.

Форма **delete** данной команды позволяет удалить интерфейс следующего транзитного узла.

Форма **show** позволяет просмотреть интерфейс следующего транзитного узла для данного маршрута.

11.2.6 protocols static route6 <ipv6-подсеть> blackhole

Настройка статического маршрута IPv6-трафика в "черную дыру".

Синтаксис

```
set protocols static route6 <ipv6-подсеть> blackhole [distance <расстояние>]
delete protocols static route6 <ipv6-подсеть> blackhole [distance]
show protocols static route6 <ipv6-подсеть> blackhole [distance]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   static {
      route6 ipv6-подсеть {
         blackhole {
            distance <расстояние>
```

```
            }
        }
    }
}
```

Параметры

ipv6-подсеть

Обязательный. Множественный узел. Определение статического маршрута. Подсеть получателя указывается в формате адрес/префикс. Чтобы определить несколько статических маршрутов, следует создать соответствующее количество узлов конфигурации route6.

расстояние

Необязательный. Указание расстояния для маршрута к «черной дыре». Чем меньше расстояние, назначенное маршруту, тем больший он имеет приоритет. Значение должно лежать в диапазоне от 1 до 255. Значение по умолчанию равно 1.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для настройки маршрута IPv6-трафика к «черной дыре». Маршрут к «черной дыре» - это маршрут, все пакеты для которого отбрасываются.

Форма **set** данной команды используется для установки маршрута IPv6-трафика к «черной дыре».

Форма **delete** используется для удаления маршрута IPv6-трафика к «черной дыре».

Форма **show** данной команды используется для просмотра настройки маршрута IPv6-трафика к «черной дыре».

11.2.7 protocols static route6 <ipv6-подсеть> next-hop <ipv6-адрес>

Установка адреса следующего узла для статического маршрута IPv6-трафика.

Синтаксис

```
set protocols static route6 <ipv6-подсеть> next-hop <ipv6-адрес> [disable | distance <расстояние> | interface <интерфейс>]

delete protocols static route6 <ipv6-подсеть> next-hop <ipv6-адрес> [disable | distance | interface]

show protocols static route6 <ipv6-подсеть> next-hop <ipv6-адрес> [disable | distance | interface]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    static {
        route6 ipv6-подсеть {
            next-hop ipv6-адрес {
                disable
                distance расстояние
                interface интерфейс
            }
        }
    }
```

```
}
```

Параметры

ipv6-подсеть

Обязательный. Множественный узел. Определение статического маршрута. Подсеть получателя указывается в формате адрес/префикс. Чтобы определить несколько статических маршрутов, следует создать соответствующее количество узлов конфигурации route6.

ipv6-адрес

Обязательный. Адрес следующего узла.

disable

Отключение статического маршрута.

расстояние

Необязательный. Установка расстояния до следующего узла для данного маршрута. Чем меньше расстояние, назначенное маршруту, тем больший он имеет приоритет. Значение должно лежать в диапазоне от 1 до 255. Значение по умолчанию равно 1.

интерфейс

Не обязательный. Имя интерфейса. В случае, если адрес следующего узла находится в диапазоне FE80::/64, то есть является link-local адресом, необходимо задать исходящий интерфейс (outgoing interface), в противном случае, произойдет ошибка, так как link-local адреса не являются уникальными.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для настройки статического маршрута IPv6-трафика.

Форма **set** данной команды позволяет указать следующий транзитный узел для данного маршрута.

Форма **delete** данной команды позволяет удалить следующий транзитный узел для статического маршрута.

Форма **show** данной команды позволяет вывести настройку следующего транзитного узла для статического маршрута.

11.2.8 protocols static table <имя_таблицы>

Определение таблицы маршрутизации.

Синтаксис

```
set protocols static table <имя_таблицы>
delete protocols static table <имя_таблицы>
show protocols static table <имя_таблицы>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   static {
      table имя_таблицы {
      }
   }
}
```

Параметры

имя_таблицы

Определение имени таблицы маршрутизации трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения таблицы маршрутизации трафика. Можно создать несколько несколько таблиц маршрутизации, создав необходимое количество узлов конфигурации table. В Numa Edge может быть одновременно создано до двухсот таблиц маршрутизации.

Форма **set** данной команды позволяет создать таблицу маршрутизации трафика.

Форма **delete** данной команды позволяет удалить таблицу маршрутизации трафика.

Форма **show** позволяет просмотреть настройки таблицы маршрутизации трафика.

11.2.9 protocols static table <имя_таблицы> dhcp <интерфейс>

Установка получения маршрутов по протоколу DHCP с указанного интерфейса.

Синтаксис

```
set protocols static table <имя_таблицы> dhcp <интерфейс>  [default-route <состояние> | static-routes <состояние>]

delete protocols static table <имя_таблицы> dhcp <интерфейс> [default-route | static-routes]

show protocols static table <имя_таблицы> dhcp <интерфейс> [default-route | static-routes]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   static {
      table имя_таблицы {
         dhcp интерфейс {
            default-route состояние
            static-routes состояние
         }
      }
   }
}
```

Параметры

имя_таблицы

Имя таблиц маршрутизации трафика.

интерфейс

Обязательный. Интерфейс, с которого будет происходить получение маршрутной информации. Интерфейс должен быть заранее сконфигурирован. Подразумевается, что интерфейс имеет настройку на DHCP.

default-route *состояние*

Включение или отключение получения адреса шлюза, переданного сервером DHCP для указанного интерфейса.

enable: Включить получение адреса шлюза по умолчанию.

disable: Отключить получение адреса шлюза по умолчанию.

static-routes *состояние*

Включение или отключение получения статических маршрутов, переданных сервером DHCP для указанного интерфейса.

enable: Включить получение статических маршрутов.

disable: Отключить получение статических маршрутов.

Значение по умолчанию

По умолчанию включено получение статических маршрутов и адреса шлюза по умолчанию.

ПРИМЕЧАНИЕ: Данное утрверждение справедливо только в том случае, если созданы узлы конфигурации
`protocols static table <имя_таблицы> dhcp <интерфейс> default-route`
либо
`protocols static table <имя_таблицы> dhcp <интерфейс> static-routes`
но для них не указано значение параметра <состояние>.
Если же данные узлы конфигурации не настроены, то маршруты, полученные от DHCP сервера, не добавляются в таблицы маршрутизации.

Указания по использованию

Эта команда используется для получения маршрутов по протоколу DHCP с указанного интерфейса.

Форма **set** данной команды позволяет указать интерфейс для получения маршрутной информации по протоколу DHCP.

Форма **delete** данной команды позволяет удалить интерфейс интерфейс для получения маршрутной информации по протоколу DHCP.

Форма **show** позволяет просмотреть интерфейс для получения маршрутной информации по протоколу DHCP.

11.2.10 protocols static table <имя_таблицы> interface-route <ipv4-подсеть> next-hop-interface <интерфейс>

Установка интерфейса следующего узла для статического маршрута таблицы маршрутизации, основанного на интерфейсе.

Синтаксис

```
set protocols static table <имя_таблицы> interface-route <ipv4-подсеть> next-hop-interface <интерфейс> [disable | distance <расстояние>]

delete protocols static table <имя_таблицы> interface-route <ipv4-подсеть> next-hop-interface <интерфейс> [disable | distance <расстояние>]

show protocols static table <имя_таблицы> interface-route <ipv4-подсеть> next-hop-interface <интерфейс> [disable | distance <расстояние>]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   static {
      table имя_таблицы {
         interface-route ipv4-подсеть {
            next-hop-interface интерфейс {
               disable
```

```
                distance расстояние
            }
        }
    }
}
```

Параметры

имя_таблицы

Имя таблицы маршрутизации трафика.

ipv4-подсеть

Обязательный. Множественный узел. Определение статического маршрута, основанного на интерфейсе. Подсеть получателя указывается в формате адрес/префикс. Чтобы создать несколько маршрутов, основанных на интерфейсе, следует создать соответствующее количество узлов конфигурации interface-route для данной таблицы маршрутизации.

интерфейс

Обязательный. Интерфейс, на который необходимо перенаправить трафик для указанной подсети. Интерфейс должен быть заранее определен в системе.

disable

Отключение статического маршрута на основе интерфейса.

расстояние

Необязательный. Установка расстояния следующего транзитного узла для данного маршрута. Чем меньше расстояние, назначенное маршруту, тем больший он имеет приоритет. Значение должно лежать в диапазоне от 1 до 255. Значение по умолчанию равно 1.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для настройки в таблице маршрутизации статического маршрута на основе интерфейса.

Форма **set** данной команды позволяет указать интерфейс следующего транзитного узла для данного маршрута в таблице маршрутизации.

Форма **delete** данной команды позволяет удалить интерфейс следующего транзитного узла для данного маршрута в таблице маршрутизации.

Форма **show** позволяет просмотреть интерфейс следующего транзитного узла для данного маршрута в таблице маршрутизации.

11.2.11 protocols static table <имя_таблицы> route <ipv4-подсеть> blackhole

Настройка статического маршрута в таблице маршрутизации в «черную дыру».

Синтаксис

```
set protocols static table <имя_таблицы> route <ipv4-подсеть> blackhole
[distance <расстояние>]

delete protocols static table <имя_таблицы> route <ipv4-подсеть> blackhole
[distance <расстояние>]

show protocols static table <имя_таблицы> route <ipv4-подсеть> blackhole
[distance]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    static {
        table имя_таблицы {
            route ipv4-подсеть {
              blackhole {
                  distance расстояние
               }
            }
        }
    }
}
```

Параметры

имя_таблицы

Имя таблицы маршрутизации трафика.

ipv4-подсеть

Обязательный. Множественный узел. Определение статического маршрута. Подсеть получателя указывается в формате адрес/префикс. Чтобы определить несколько статических маршрутов, следует создать соответствующее количество узлов конфигурации route для данной таблицы маршрутизации.

расстояние

Необязательный. Указание расстояния для маршрута к «черной дыре». Чем меньше расстояние, назначенное маршруту, тем больший он имеет приоритет. Значение должно лежать в диапазоне от 1 до 255. Значение по умолчанию равно 1.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для настройки маршрута к «черной дыре». Маршрут к «черной дыре» — это маршрут, все пакеты для которого отбрасываются.

Форма **set** данной команды используется для установки маршрута к «черной дыре» в данной таблице маршрутизации.

Форма **delete** используется для удаления маршрута к «черной дыре» в данной таблице маршрутизации.

Форма **show** данной команды используется для просмотра настройки маршрута к «черной дыре» в данной таблице маршрутизации.

11.2.12 protocols static table <имя_таблицы> route <ipv4-подсеть> next-hop <ipv4-адрес>

Установка следующего узла статического маршрута таблицы маршрутизации.

Синтаксис

```
set protocols static <имя_таблицы> route <ipv4-подсеть> next-hop <ipv4-адрес> [disable | distance <расстояние>]

delete protocols static <имя_таблицы> route <ipv4-подсеть> next-hop <ipv4-адрес> [disable | distance <расстояние>]

show protocols static <имя_таблицы> route <ipv4-подсеть> next-hop <ipv4-адрес> [disable | distance <расстояние>]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   static {
      table имя_таблицы {
         route ipv4-подсеть {
            next-hop ipv4-адрес {
               disable
              distance расстояние
            }
         }
      }
   }
}
```

Параметры

имя_таблицы

Имя таблицы маршрутизации трафика.

ipv4-подсеть

Обязательный. Множественный узел. Определение статического маршрута. Подсеть получателя указывается в формате адрес/префикс. Чтобы определить несколько статических маршрутов, следует создать соответствующее количество узлов конфигурации **route** для данной таблицы маршрутизации.

ipv4-адрес

Обязательный. Адрес следующего узла.

disable

Отключение статического маршрута.

расстояние

Необязательный. Установка расстояния следующего транзитного узла для данного маршрута. Чем меньше расстояние, назначенное маршруту, тем больший он имеет приоритет. Значение должно лежать в диапазоне от 1 до 255. Значение по умолчанию равно 1.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для настройки статического маршрута в таблице маршрутизации трафика.

Форма **set** данной команды позволяет указать следующий транзитный узел для данного маршрута.

Форма **delete** данной команды позволяет удалить следующий транзитный узел для статического маршрута в таблице маршрутизации.

Форма **show** данной команды позволяет вывести настройку следующего транзитного узла для статического маршрута в таблице маршрутизации.

11.2.13 policy clear prefix-list

Очистка статистики или состояния для списка префиксов.

Синтаксис

```
policy clear prefix-list [<список> [<префикс_подсети_ipv4>]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

список

Необязательный. Очистка статистики для указанного списка префиксов.

префикс_подсети_ipv4

Необязательный. Очистка статистики для указанной подсети.

Значение по умолчанию

Статистика очищается для всех списков префиксов.

Указания по использованию

Команда позволяет очистить статистические данные или состояния для списка префиксов.

11.2.14 clear ip route cache

Очистка кэша маршрутизации ядра для протокола IPv4.

Синтаксис

```
clear ip route cache [<префикс_подсети_ipv4>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

префикс_подсети_ipv4

Необязательный. Удаление указанного маршрута из кэша маршрутизации ядра.

Значение по умолчанию

Очистка всего кэша маршрутизации.

Указания по использованию

Команда используется для очистки кэша маршрутизации ядра или для удаления конкретного маршрута из кэша.

11.2.15 show ip forwarding

Отображение состояния пересылки пакетов для протокола IPv4.

Синтаксис

```
show ip forwarding
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для отображения текущего состояния пересылки пакетов IP.

Примеры

В примере приведен вывод сведений о состоянии пересылки пакетов IP.

Пример 109– Отображение состояния пересылки пакетов IP

```
admin@edge:~$ show ip forwarding
IP forwarding is on
```

```
admin@edge:~$
```

11.2.16 show ip route

Отображение маршрутов, содержащихся в таблице маршрутизации и таблице пересылки для протокола IPv4.

Синтаксис

```
show ip route [<ipv4-адрес> |<префикс_подсети_ipv4> [<longer-prefixes>]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

ipv4-адрес

Необязательный. Отображение сведений о маршруте для указанного адреса.

префикс_подсети_ipv4

Необязательный. Отображение сведений о маршруте для указанного префикса.

longer-prefixes

Необязательный. Отображение сведений о маршрутах с большим префиксом подсети.

Значение по умолчанию

Отображение всех маршрутов из таблицы маршрутизации и таблицы пересылки.

Указания по использованию

Команда используется для просмотра маршрутов, которые содержатся в таблице маршрутизации (Routing Information Base, RIB) и таблице пересылки (Forwarding Information Base, FIB).

Примеры

В примере ниже приведен образец вывода маршрутов из таблицы маршрутизации и таблицы пересылки.

Пример 110– Отображение маршрутов из таблицы маршрутизации и таблицы пересылки

```
admin@edge:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
       > - selected route, * - FIB route

C>* 127.0.0.0/8 is directly connected, lo
C>* 192.168.12.0/24 is directly connected, eth2
C>* 192.168.13.0/24 is directly connected, eth1
S>* 192.168.20.0/24 [1/0] via 192.168.12.254, eth2
S>* 192.168.30.0/24 [1/0] via 192.168.13.254, eth1
S>* 192.168.30.1/32 [1/0] via 192.168.13.254, eth1
admin@edge:~$
```

В примере ниже приведен образец вывода маршрута до IP-адреса 192.168.20.25.

Пример 111– Отображение маршрутов, касающихся указанного адреса

```
admin@edge:~$ show ip route 192.168.20.25
Routing entry for 192.168.20.0/24
  Known via "static", distance 1, metric 0, tag 0, vrf 0, best, fib
  >* 192.168.12.254, via eth2

admin@edge:~$
```

В примере ниже приведен образец вывода маршрутов с большим префиксом, чем 192.168.30.0/24

Пример 112– Отображение маршрутов с большей маской подсети

```
admin@edge:~$ show ip route 192.168.30.0/24 longer-prefixes
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
       > - selected route, * - FIB route

S>* 192.168.30.0/24 [1/0] via 192.168.13.254, eth1
S>* 192.168.30.1/32 [1/0] via 192.168.13.254, eth1
admin@edge:~$
```

11.2.17 show ip route cache

Отображение кэша маршрутизации ядра для протокола IPv4.

Синтаксис

```
show ip route cache <префикс_подсети_ipv4>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

префикс_подсети_ipv4

Необязательный. Отображение сведений об указанном маршруте из кэша маршрутизации ядра.

Значение по умолчанию

Отображение всех маршрутов из кэша маршрутизации ядра.

Указания по использованию

Команда позволяет отобразить маршруты, хранящиеся в кэше маршрутизации ядра. В кэше маршрутизации хранятся все маршруты, используемые кэшем в данный момент.

ПРИМЕЧАНИЕ. Кэш маршрутизации может быть отключен в используемой версии ядра. В таком случае будет выведен соответствующее сообщение пользователю.

11.2.18 show ip route connected

Отображение маршрутов, подключенных напрямую для протокола IPv4.

Синтаксис

```
show ip route connected
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для отображения маршрутов, подключенных напрямую к системе Numa Edge.

Примеры

В примере приведен вывод маршрутов, подключенных напрямую.

Пример 113– Отображение маршрутов, подключенных напрямую

```
admin@edge:~$ show ip route connected
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
       > - selected route, * - FIB route

C>* 127.0.0.0/8 is directly connected, lo
C>* 192.168.12.0/24 is directly connected, eth2
C>* 192.168.13.0/24 is directly connected, eth1
admin@edge:~$
```

11.2.19 show ip route forward

Отображение маршрутов, которые содержатся в таблице пересылки (Forwarding Information Base, FIB) для протокола IPv4.

Синтаксис

```
show ip route forward <префикс_подсети_ipv4>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

префикс_подсети_ipv4

Необязательный. Отображение сведений из таблицы пересылки ядра для указанного маршрута.

Значение по умолчанию

Отображение маршрутов, которые содержатся в таблице пересылки.

Указания по использованию

Эта команда используется для отображения таблицы пересылки.

В том случае если определены маршруты с равной стоимостью, они также содержатся в таблице пересылки. До того, как может быть выполнена маршрутизация по алгоритму ECMP (Equal-Cost-Multi-Path), необходимо иметь несколько путей с равной стоимостью.

Примеры

В примере ниже показано, как отобразить маршруты, записанные в таблице пересылки.

Пример 114– Отображение маршрутов из таблицы пересылки

```
admin@edge:~$ show ip route forward
192.168.12.0/24 dev eth2  proto kernel  scope link  src 192.168.12.1
192.168.13.0/24 dev eth1  proto kernel  scope link  src 192.168.13.1
192.168.20.0/24 via 192.168.12.254 dev eth2  proto zebra  metric 20
192.168.30.0/24 via 192.168.13.254 dev eth1  proto zebra  metric 20
192.168.30.1 via 192.168.13.254 dev eth1  proto zebra  metric 20
192.168.200.0/24 dev ethm  proto kernel  scope link  src 192.168.200.1
linkdown
admin@edge:~$
```

В примере ниже показано, как отобразить сведения о маршруте 10.1.0.0/24 из таблицы пересылки.

Пример 115– Отображение сведений о маршруте из таблицы пересылки

```
admin@edge:~$ show ip route forward 192.168.30.0/24
192.168.30.0/24 via 192.168.13.254 dev eth1  proto zebra  metric 20
admin@edge:~$
```

11.2.20 show ip route kernel

Отображение маршрутов ядра для протокола IPv4.

Синтаксис

```
show ip route kernel
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения маршрутов ядра. К маршрутам ядра относятся маршруты, которые были добавлены напрямую в ядро, например с помощью команды route add:

route add -net 192.168.50.0 netmask 255.255.255.0 gw 192.168.15.254

Примеры

В примере показано, как отобразить маршруты ядра.

Пример 116– Отображение маршрутов ядра

```
admin@edge:~$ show ip route kernel
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
       > - selected route, * - FIB route

K * 192.168.50.0/24 via 192.168.15.254, eth3 inactive
admin@edge:~$
```

11.2.21 show ip route static

Отображение статических маршрутов для протокола IPv4.

Синтаксис

```
show ip route static
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения статических маршрутов из таблицы маршрутизации.

Примеры

В примере показано, как вывести список статических маршрутов.

Пример 117– Отображение списка статических маршрутов

```
admin@edge:~$ show ip route static
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
       > - selected route, * - FIB route

S>* 192.168.20.0/24 [1/0] via 192.168.12.254, eth2
```

```
S>* 192.168.30.0/24 [1/0] via 192.168.13.254, eth1
S>* 192.168.30.1/32 [1/0] via 192.168.13.254, eth1
admin@edge:~$
```

11.2.22 show ip route summary

Отображение кратких сведений о маршрутах для протокола IPv4.

Синтаксис

```
show ip route summary
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения сводной информации о различных маршрутах.

Примеры

В примере показано, как вывести сводную информацию о маршрутах.

Пример 118– Отображение сводной информации о маршрутах

```
admin@edge:~$ show ip route summary
Route Source         Routes               FIB  (vrf 0)
kernel               1                    1
connected            3                    3
static               3                    3
------
Totals               7                    7

admin@edge:~$
```

11.2.23 show ip route supernets-only

Отображение маршрутов вышестоящих сетей для протокола IPv4.

Синтаксис

```
show ip route supernets-only
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения маршрутов вышестоящих сетей.

К маршрутам вышестоящих сетей относятся маршруты, имеющие маску подсети меньшей длины, чем стандартная маска классовой модели.

Примеры

В примере показано, как вывести список маршрутов вышестоящих сетей.

Пример 119– Отображение маршрутов вышестоящих сетей

```
admin@edge:~$ show ip route supernets-only
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
       > - selected route, * - FIB route

S>* 0.0.0.0/0 [1/0] via 192.168.12.254, eth2
admin@edge:~$
```

11.2.24 clear ipv6 neighbors

Очистка кэша протокола обнаружения соседей.

Синтаксис

```
clear ipv6 neighbours [address <ipv6-адрес> | interface <интерфейс>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

ipv6-адрес

Удаление кэша протокола обнаружения соседей для указанного адреса IPv6.

интерфейс

Удаление кэша протокола обнаружения соседей для указанного интерфейса.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для очистки кэша протокола обнаружения соседей для указанного адреса или интерфейса системы.

11.2.25 clear ipv6 route cache

Очистка кэша маршрутизации ядра для протокола IPv6.

Синтаксис

```
clear ipv6 route cache <префикс_подсети_ipv6>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

префикс_подсети_ipv6

Необязательный. Удаление указанного маршрута из кэша маршрутизации ядра.

Значение по умолчанию

Очистка всего кэша маршрутизации.

Указания по использованию

Команда используется для очистки кэша маршрутизации ядра или для удаления конкретного маршрута из кэша.

11.2.26 show ipv6 forwarding

Отображение состояния пересылки пакетов для протокола IPv6.

Синтаксис

```
show ipv6 forwarding
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для отображения текущего состояния пересылки пакетов IP.

11.2.27 show ipv6 neighbors

Отображение кэша протокола обнаружения соседей.

Синтаксис

```
show ipv6 neighbours
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отображение информации из кэша протокола обнаружения соседей.

Указания по использованию

Команда используется для просмотра кэша протокола обнаружения соседей.

11.2.28 show ipv6 route

Отображение маршрутов, содержащихся в таблице маршрутизации и таблице пересылки для протокола IPv6.

Синтаксис

```
show ipv6 route [<ipv6-адрес> | <префикс_подсети_ipv6> [<longer-prefixes>]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

ipv6-адрес

Необязательный. Отображение сведений о маршруте для указанного адреса.

префикс_подсети_ipv6

Необязательный. Отображение сведений о маршруте для указанного префикса.

longer-prefixes

Необязательный. Отображение сведений о маршрутах с большим префиксом подсети.

Значение по умолчанию

Отображение всех маршрутов из таблицы маршрутизации и таблицы пересылки.

Указания по использованию

Команда используется для просмотра маршрутов, которые содержатся в таблице маршрутизации (Routing Information Base, RIB) и таблице пересылки (Forwarding Information Base, FIB).

11.2.29 show ipv6 route cache

Отображение кэша маршрутизации ядра для протокола IPv6.

Синтаксис

```
show ipv6 route cache <префикс_подсети_ipv6>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

префикс_подсети_ipv6

Необязательный. Отображение сведений об указанном маршруте из кэша маршрутизации ядра.

Значение по умолчанию

Отображение всех маршрутов из кэша маршрутизации ядра.

Указания по использованию

Команда позволяет отобразить маршруты, хранящиеся в кэше маршрутизации ядра. В кэше маршрутизации хранятся все маршруты, используемые кэшем в данный момент.

11.2.30 show ipv6 route connected

Отображение маршрутов, подключенных напрямую для протокола IPv6.

Синтаксис

```
show ipv6 route connected
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для отображения маршрутов, подключенных напрямую к системе Numa Edge.

11.2.31 show ipv6 route forward

Отображение маршрутов, которые содержатся в таблице пересылки (Forwarding Information Base, FIB) для протокола IPv6.

Синтаксис

```
show ipv6 route forward <префикс_подсети_ipv6>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

префикс_подсети_ipv6

Необязательный. Отображение сведений из таблицы пересылки ядра для указанного маршрута.

Значение по умолчанию

Отображение маршрутов, которые содержатся в таблице пересылки.

Указания по использованию

Эта команда используется для отображения таблицы пересылки.

В том случае если определены маршруты с равной стоимостью, они также содержатся в таблице пересылки. До того, как может быть выполнена маршрутизация по алгоритму ECMP (Equal-Cost-Multi-Path), необходимо иметь несколько путей с равной стоимостью.

11.2.32 show ipv6 route kernel

Отображение маршрутов ядра для протокола IPv6.

Синтаксис

```
show ipv6 route kernel
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения маршрутов ядра. К маршрутам ядра относятся маршруты, которые были добавлены напрямую в ядро, например с помощью команды route add.

11.2.33 show ipv6 route static

Отображение статических маршрутов для протокола IPv6.

Синтаксис

```
show ipv6 route static
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения статических маршрутов из таблицы маршрутизации.

11.2.34 show ipv6 route summary

Отображение кратких сведений о маршрутах для протокола IPv6.

Синтаксис

```
show ipv6 route summary
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения сводной информации о различных маршрутах.

11.2.35 routing table show

Отображение таблицы маршрутизации системы.

Синтаксис

```
routing table show [<имя_таблицы> [route | statistics]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_таблицы

Имя таблицы маршрутизации. Используется совместно с параметрами route или statistics.

route

Отображение маршрутов в указанной таблице маршрутизации.

statistics

Отображение статистики по указанной таблице маршрутизации.

Значение по умолчанию

Выводит список таблиц маршрутизации, созданных с помощью команды protocols static table.

Указания по использованию

Эта команда используется для отображения пользовательских таблиц маршрутизации Numa Edge.

Примеры

В примере показано, как вывести таблицу маршрутизации.

Пример 120– Отображение таблицы маршрутизации

```
admin@edge:~$ routing table show test_table route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
       > - selected route, * - FIB route

K>* 0.0.0.0/0 [table test_table] via 192.168.11.254, eth1
C>* 127.0.0.0/8 [table test_table] is directly connected, lo
C>* 192.168.11.0/24 [table test_table] is directly connected, eth1
admin@edge:~$
```

12 Инфраструктура открытых ключей

В систему Numa Edge входит модуль управления PKI (инфраструктурой открытых ключей), предоставляющий сервисы для использования технологии открытых ключей. Универсальное применение сертификатов обеспечивает стандарт Международного Союза по телекоммуникациям X.509, который является базовым и поддерживается целым рядом протоколов безопасности. В их числе — стандарты шифрования и ЭЦП с открытыми ключами, протокол связи SSL и безопасный протокол передачи гипертекстовых сообщений HTTPS (Secure HTTP). Модуль PKI предназначен для выпуска и управления сертификатами, создания пары ключей (открытый и закрытый) для шифрования данных, управления базой данных инфраструктуры открытых ключей.

Сервисы, предоставляемые модулем PKI могут быть использованы при настройке аутентификации узлов VPN на базе сертификатов X.509, а также при настройке аутентификации пользователей системы Numa Edge.

Сервисы управления PKI реализованы на базе библиотеки OpenSSL.

Сервисы управления предоставляют возможности по созданию сертификата пользователя и его подписание на базе российских криптографических алгоритмов (функции хеширования ГОСТ Р34.11-2012, цифровой подписи — ГОСТ Р34.10-2012 и ГОСТ Р34.10-2001 для обратной совместимости), а также на базе криптосистемы RSA. Цифровые сертификаты соответствуют международным рекомендациям X.509 v3 и могут выдаваться в форматах PKCS12 или PEM.

В процессе управления ключами УЦ имеет возможность отзыва выпущенных им сертификатов, что необходимо для досрочного прекращения их действия, например, в случае компрометации ключа.

ПРИМЕЧАНИЕ. В связи с ограниченным функционалом УЦ, встроенного в Numa Edge, рекомендуется использовать сторонние УЦ.

12.1 Основные компоненты PKI

Неотъемлемым компонентом инфраструктуры открытых ключей является удостоверяющий центр. Непосредственное использование открытых ключей требует дополнительной их защиты и идентификации для определения связи с секретным ключом. Электронный сертификат представляет собой цифровой документ, который связывает открытый ключ с его владельцем. Для заверения электронного сертификата используется электронная цифровая подпись удостоверяющего центра (УЦ). УЦ включает свое имя в каждый выпущенный им сертификат и подписывает их при помощи собственного секретного ключа. Конечные субъекты идентифицируют сертификаты по имени УЦ, и могут убедиться в их подлинности, используя его открытый ключ.

Удостоверяющий центр выполняет следующие основные функции:

- формирует собственный секретный ключ и самоподписанный сертификат;
- выпускает сертификаты сервера и клиентов;
- ведет базу данных всех изданных сертификатов и формирует список аннулированных сертификатов.

Инфраструктура открытых ключей позволяет генерировать пары ключей (открытый ключ/секретный ключ). Генерация ключей может осуществляться централизованно (удостоверяющим центром) или индивидуально (конечным субъектом). В том случае если генерация ключей осуществляется конечными пользователями, они должны иметь соответствующие программные или аппаратные средства для создания надежных ключей. В том случае если пользователь не предъявляет достаточных мер для защиты своих секретных ключей, инфраструктура PKI подвергается серьезному риску.

К преимуществам централизованной генерации можно отнести быстроту создания ключей, использование специализированных средств генерации высококачественных ключей, контроль соответствия алгоритмов генерации установленным стандартам, а также хранение резервных копий на случай их утери пользователями. В том случае если ключи генерируются централизованно, они должны транспортироваться пользователям только через безопасные каналы связи.

В том случае если секретный ключ пользователя потерян, похищен или скомпрометирован, или если есть вероятность наступления таких событий, действие сертификата должно быть прекращено.

Формат сертификата определен в рекомендациях Международного союза по телекоммуникациям ITU (X.509), в настоящее время основным используемым форматом является формат версии 3.

Сертификат представляет собой структурированную двоичную запись, содержащую элементы данных, сопровождаемые цифровой подписью издателя сертификата. В сертификате имеется десять основных полей: шесть обязательных и четыре опциональных. К обязательным полям относятся:

- идентификатор алгоритма подписи Signature Algorithm Identifier;
- имя издателя Issuer Name;
- период действия Validity (Not before / After);
- открытый ключ субъекта Subject Public Key Information;
- имя субъекта сертификата Subject Name.

В данном случае под субъектом понимается сторона, контролирующая секретный ключ, соответствующий данному открытому ключу.

Поле Version задает синтаксис сертификата. Удостоверяющий центр, выпускающий сертификат, присваивает каждому сертификату серийный номер Certificate Serial Number, который должен быть уникален.

В поле Signature Algorithm Identifier указывается идентификатор алгоритма ЭЦП, который был использован для защиты сертификата. В поле Validity (Not Before/After) указываются даты начала и окончания периода действия сертификата.

Каждый раз при использовании сертификата проверяется, является ли сертификат действующим. Сертификаты, срок действия которых истек, должны аннулироваться удостоверяющим центром.

12.2 Особенности реализации PKI

12.2.1 Организация хранения сертификатов

В Numa Edge все сертификаты УЦ и конечные сертификаты хранятся в одной директории. В связи с этим накладываются определенные ограничения на именование сертификатов.

С точки зрения системы конфигурирования, имена сертификатов в файловой системе представляют собой имена узлов ca <имя> и certificate <имя_сертификата>.

В конфигурационном режиме накладываемые ограничения выражаются в невозможности указать одинаковые имена для узлов УЦ или конечных сертификатов. В таком случае для сертификата УЦ выполняемые действия будут рассматриваться как попытка изменить существующий сертификат, что запрещено, а для конечного сертификата (например, в рамках соседнего УЦ) будет выдано соответствующее предупреждение на стадии commit вида:

```
E: Сертификат с именем 'TestCert' уже существует
Commit failed
```

При импорте сертификатов также следует учитывать существующие ограничения. При попытке импорта сертификата УЦ, с именем, идентичным уже имеющемуся в системе, будет выдано предупреждение вида:

```
Импортируется сертификат УЦ CA Certificate как CACert
E: Существует другой УЦ с таким же именем CACert
```

ПРИМЕЧАНИЕ С конечными сертификатами подобное ограничение для операции импорта отсутствует. Таким образом, можно заменить конечный сертификат в рамках уже имеющегося другого или того же УЦ, в случае совпадения их имён. Следует обращать внимание на эту особенность перед выполнением импорта сертификатов.

12.2.2 Совместимость реализации PKI

При экспорте ключей из Numa Edge в сторонние устройства могут возникнуть проблемы совместимости. Например, если есть сервер OpenLDAP, собранный с поддержкой библиотеки GnuTLS (а не OpenSSL), то при экспортировании созданного на Numa Edge сертификата и использовании его в качестве сертификата сервера, сервер OpenLDAP не будет запущен и будет получено следующее сообщение об ошибке:

```
TLS init def ctx failed: -207
```

Данная ситуация обусловлена тем, что секретный ключ при генерации сертификата на Numa Edge создается в формате PKCS#8, который не поддерживается сервером OpenLDAP, собранным с поддержкой GnuTLS. Для конвертации секретного ключа в традиционный формат необходимо воспользоваться следующей командой:

```
openssl rsa -in old_key.pem -out new_key.pem
```

12.3 Пример настройки PKI

В этом наборе примеров приведено создание инфраструктуры открытых ключей в системе Numa Edge, генерация сертификатов, экспорт/импорт сертификатов. В данном наборе примеров используются две системы Numa Edge, имеющие имена edge1 и edge2 соответственно.

12.3.1 Создание удостоверяющего центра

В данном примере будет приведено создание удостоверяющего центра, который будет использован для управления сертификатами стандарта X.509.

В данном примере удостоверяющий центр создается на узле edge1. На базе созданного удостоверяющего центра будет осуществляться централизованное создание и управление ключевыми парами и сертификатами узлов edge1 и edge2. Для создания нового удостоверяющего центра необходимо выполнить следующие шаги на узле edge1 в режиме настройки.

Пример 121– Создание удостоверяющего центра на узле edge1

Действие	**Команда**
Создание удостоверяющего центра	`[edit]` `admin@edge1# set pki ca MainCA`
Указание общего имени (common name) удостоверяющего центра	`[edit]` `admin@edge1# set pki ca MainCA cn "Main Certification Authority"`
Указание города, в качестве одного из атрибутов идентификатора УЦ	`[edit]` `admin@edge1# set pki ca MainCA city SPb`
Указание страны, в качестве одного из атрибутов идентификатора УЦ	`[edit]` `admin@edge1# set pki ca MainCA country RU`
Указание периода действия сертификата удостоверяющего центра	`[edit]` `admin@edge1# set pki ca MainCA expiration 365`
Фиксация настройки	`[edit]` `admin@edge1# commit`

Вывод настройки	`[edit]`
	`admin@edge1# show pki ca MainCA`
	`  city SPb`
	`  cn "Main Certification Authority"`
	`  country RU`
	`  expires-on "Thu Nov 7 12:35:42 2020"`
	`  key-size 256`
	`  key-type gost2012`

12.3.2 Генерация сертификата узла edge1

В данном примере будет приведено создание сертификата узла edge1.

Для создания сертификата узла edge1 необходимо выполнить следующие шаги на узле edge1 в режиме настройки.

Пример 122– Создание сертификата узла edge1

Действие	**Команда**
Создание сертификата для узла edge1	`[edit]` `admin@edge1# set pki ca MainCA certificate edge1-cert`
Указание общего имени (common name), которое будет указано в сертификате узла edge1	`[edit]` `admin@edge1# set pki ca MainCA certificate edge1-cert cn "edge1 VPN certificate"`

Указание срока действия сертифката. Срок действия выпускаемого сертификата не должен превышать срок сдейтсвия сертификата УЦ.	[edit] admin@edge1# set pki ca MainCA certificate edge1-cert expiration 180
Фиксация настройки	[edit] admin@edge1# commit
Вывод настройки созданного сертификата	[edit] admin@edge1# show pki ca MainCA certificate edge1-cert cn "edge1 VPN certificate" expires-on "Mon May 6 12:37:11 2020" key-size 256 key-type gost2012

12.3.3 Генерация сертификата узла edge2

В данном примере будет приведено создание сертификата узла edge2.

Для создания сертификата узла edge2 необходимо выполнить следующие шаги на узле edge1 в режиме настройки.

Пример 123– Создание сертификата узла edge2

Действие	**Команда**
Создание сертификата для узла edge2	[edit] admin@edge1# set pki ca MainCA certificate edge2-cert
Указание общего имени (common name), которое будет указано в сертификате узла edge2	[edit] admin@edge1# set pki ca MainCA certificate edge2-cert cn "edge2 VPN certificate"
Указание срока действия сертифката. Срок действия выпускаемого сертификата не должен превышать срок сдейтсвия сертификата УЦ.	[edit] admin@edge1# set pki ca MainCA certificate edge2-cert expiration 180
Фиксация настройки	[edit] admin@edge1# commit
Вывод настройки созданного сертификата	[edit] admin@edge1# show pki ca MainCA certificate edge2-cert cn "edge2 VPN certificate" expires-on "Mon May 6 12:37:57 2020" key-size 256 key-type gost2012

12.3.4 Экспорт сертификата узла edge2

В данном примере приведен экспорт сертификата узла edge2 на флэш-накопитель. При выполнении команды **pki export certificate** <имя> к устройству должен быть подключен флэш-накопитель. Монтирование и размонтирование флэш-накопителя осуществляется автоматически. Экспортируемые файлы будут помещены в корневую директорию флэш-накопителя. К экспортируемым файлам относятся: сертификат удостоверяющего центра, сертификат клиента, подписанный указанным удостоверяющим центром, секретный ключ клиента и файл, содержащий список аннулированных сертификатов.

ПРИМЕЧАНИЕ При использовании команды **pki export certificate** <имя> экспортируется секретный ключ, связанный с открытым ключом, указанным в сертификате. Секретный ключ должен храниться в тайне, и не должен передаваться третьим лицам.

Для экспортирования сертификата узла edge2 на флэш-накопитель необходимо выполнить следующие шаги на узле edge1 в эксплуатационном режиме, к устройству должен быть заранее подключен флэш-накопитель.

Пример 124– Экспортирование сертификата узла edge2

Действие	Команда
Экспортирование сертификата узла edge2, секретного ключа узла edge2, сертификата удостоверяющего центра	`admin@edge1:~$ pki export certificate`

После осуществления экспорта в корневой директории флэш-накопителя будут содержаться следующие файлы:

- MainCA.crt: сертификат удостоверяющего центра;
- edge1-cert.crt: сертификат узла edge2;
- MainCA.crl: список отозванных сертификатов;
- edge2-cert.key: секретный ключ узла edge2.

12.3.5 Импорт сертификата узла edge2

В данном примере приведен импорт сертификата узла edge2 с флэш-накопителя. При выполнении команды **pki import** к устройству должен быть подключен флэш-накопитель, в корне которого должны размещаться следующие файлы:

- сертификат удостоверяющего центра;
- сертификат узла edge2;
- список отозванных сертификатов;
- секретный ключ узла edge2.

Монтирование и размонтирование флэш-накопителя осуществляется автоматически. В результате выполнения указанной команды в систему на узле edge2 будут добавлены сертификат удостоверяющего центра, сертификат узла edge2, подписанный указанным удостоверяющим центром, секретный ключ, а также файл, содержащий список аннулированных сертификатов.

Для импорта сертификата узла edge2 необходимо выполнить следующие шаги на узле edge2 в эксплуатационном режиме, к устройству должен быть заранее подключен флэш-накопитель.

Пример 125– Импорт сертификата узла edge2

Действие	Команда

Импорт сертификата узла edge2, секретного ключа узла edge2, сертификата удостоверяющего центра, списка отозванных сертификатов	`admin@edge2:~$ pki import`
	`Импортируется сертификат УЦ Main Certification Authority как MainCA`
	`Импортируется сертификат edge2 VPN certificate как edge2-cert`
	`Импортируется CRL для MainCA`
	`Импортируется ключ для edge2-cert`

Вывод секции pki в режиме конфигурирования	`[edit]`
	`admin@edge2# show pki ca MainCA`
	`certificate edge2-cert {`
	`cn "edge2 VPN certificate"`
	`expires-on "Mon May 6 12:37:57 2020"`
	`key-size 256`
	`key-type gost2012`
	`}`
	`city SPb`
	`cn "Main Certification Authority"`
	`country RU`
	`expires-on "Thu Nov 7 12:35:42 2020"`
	`key-size 256`
	`key-type gost2012`

12.4 Команды управления PKI

Команды настройки	
pki ca <имя>	Определение удостоверяющего центра
pki ca <имя> city <город>	Указание названия города, которое входит в идентификатор УЦ

pki ca <имя> cn <общее_имя>	Указание общего имени (common name), в качестве одного из атрибутов идентификатора УЦ
pki ca <имя> country <страна>	Указание названия страны, в качестве одного из атрибутов идентификатора УЦ
pki ca <имя> crldp <адрес>	Указание адреса точки распространения списка отзывов сертификатов УЦ
pki ca <имя> email <email>	Указание адреса электронной почты, в качестве одного из атрибутов идентификатора УЦ
pki ca <имя> expiration <количество_дней>	Указание количества дней, в течение которого будет действителен сертификат УЦ
pki ca <имя> expires-on <окончание_периода_действия>	Указывает дату и время окончания периода действия сертификата удостоверяющего центра
pki ca <имя> key-curve <название_кривой>	Указание названия ECDSA-кривой
pki ca <имя> key-size <длина_ключа>	Указание длины используемого ключа
pki ca <имя> key-type <тип_ключа>	Указание используемого для защиты данных криптографического алгоритма
pki ca <имя> last-update <последнее_обновление_CRL>	Указывает дату и время последнего обновления CRL для данного УЦ.
pki ca <имя> next-update <окончание_срока_действия_CRL>	Указывает дату и время окончания периода действия CRL для данного УЦ.
pki ca <имя> organization <организация>	Указание названия организации, в качестве одного из атрибутов идентификатора УЦ
pki ca <имя> organization-unit <подразделение>	Указание названия подразделения, в качестве одного из атрибутов идентификатора УЦ
pki ca <имя> province <регион>	Указание названия региона, в качестве одного из атрибутов идентификатора УЦ
pki ca <имя> certificate <имя_сертификата>	Определение сертификата, подписанного указанным удостоверяющим центром
pki ca <имя> certificate <имя_сертификата> alternative-name email <email>	Указание адреса электронной почты в качестве атрибута расширения альтернативного имени субъекта
pki ca <имя> certificate <имя_сертификата> alternative-name idn <доменное_имя>	Указание международного доменного имени в качестве атрибута расширения альтернативного имени субъекта
pki ca <имя> certificate <имя_сертификата> alternative-name ip-address <ip-адрес>	Указание IP-адреса в качестве атрибута расширения альтернативного имени субъекта
pki ca <имя> certificate <имя_сертификата> city <город>	Указание названия города, в качестве одного из атрибутов идентификатора субъекта
pki ca <имя> certificate <имя_сертификата> cn <общее_имя>	Указание общего имени, которое входит в идентификатор субъекта
pki ca <имя> certificate <имя_сертификата> country <страна>	Указание названия страны, в качестве одного из атрибутов идентификатора субъекта
pki ca <имя> certificate <имя_сертификата> email <email>	Указание адреса электронной почты, в качестве одного из атрибутов идентификатора субъекта
pki ca <имя> certificate <имя_сертификата> expiration <количество_дней>	Указание количества дней, в течение которого будет действителен указанный сертификат
pki ca <имя> certificate <имя_сертификата> expires-on <окончание_периода_действия>	Указание даты и времени окончания периода действия данного сертификата
pki ca <имя> certificate <имя_сертификата> organization <подразделение>	Указание названия организации, в качестве одного из атрибутов идентификатора субъекта
pki ca <имя> certificate <имя_сертификата> organization-unit <подразделение>	Указание названия подразделения, в качестве одного из атрибутов идентификатора субъекта
pki ca <имя> certificate <имя_сертификата> province <регион>	Указание названия региона, в качестве одного из атрибутов идентификатора субъекта
pki ca <имя> certificate <имя_сертификата> usage	Указание ограничений по использованию сертификата в

<сторона> <состояние>	расширении X509v3
Эксплуатационные команды	
pki export ca <имя> crl <формат>	Экспорт файла со списком отозванных сертификатов в указанном формате
pki export certificate <имя_сертификата>	Экспорт сертификата субъекта, ключевой пары субъекта, сертификата УЦ, списка отозванных сертификатов
pki export-pkcs12 certificate <имя_сертификата> password <пароль>	Экспорт сертификата субъекта, ключевой пары субъекта, сертификата УЦ, списка отозванных сертификатов в формате PKCS12
pki import	Импорт сертификата/сертификатов УЦ, сертификата субъекта, ключевой пары субъекта, сертификата УЦ, списка отозванных сертификатов.
pki import-pkcs12 password <пароль>	Импорт сертификата субъекта, ключевой пары субъекта, сертификата УЦ в формате PKCS12 и списка отозванных сертификатов
pki revoke ca <имя> certificate <имя_сертификата>	Команда для отзыва сертификата
pki update-crl	Обновление списка отозванных сертификатов для УЦ, в сертификате которых присутствует расширение CRLDistributionPoints

12.4.1 pki ca <имя>

Определение удостоверяющего центра.

Синтаксис

```
set pki ca <имя>
delete pki ca <имя>
show pki ca <имя>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
    }
}
```

Параметры

имя

Множественный. Название узла конфигурации определяемого удостоверяющего центра. Можно определить несколько удостоверяющих центров, создав соответствующее количество узлов конфигурации.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для создания удостоверяющего центра и указания названия его узла конфигурации.

Форма **set** данной команды используется для создания удостоверяющего центра.

Форма **delete** данной команды используется для удаления настройки удостоверяющего центра.

Форма **show** данной команды используется для отображения настройки удостоверяющего центра.

12.4.2 pki ca <имя> city <город>

Указание названия города, в качестве одного из атрибутов идентификатора УЦ.

Синтаксис

```
set pki ca <имя> city <город>
delete pki ca <имя> city
show pki ca <имя> city
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
   ca имя {
      city город
   }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

город

Название города. В том случае если название содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать название города, которое входит в идентификатор удостоверяющего центра. Идентификатор удостоверяющего центра представляет собой отличительное имя удостоверяющего центра в формате X.500, и состоит из набора иерархических атрибутов, в состав которых могут входить общее имя УЦ, адрес электронной почты, название организации и подразделения организации, атрибутов месторасположения таких как название страны, региона, города.

Указание названия города не является обязательным.

ПРИМЕЧАНИЕ Значения параметров УЦ, в том числе атрибутов идентификатора УЦ, не могут быть изменены после фиксации настройки. Для того чтобы изменить значения параметров УЦ, необходимо удалить настройку УЦ и создать ее заново, при этом для УЦ будет создана новая ключевая пара, соответственно с точки зрения системы, вновь созданный УЦ, даже при полном соответствии значений параметров, будет являться новым УЦ, отличным от предыдущего. Таким образом, сертификаты выпущенные до этого будут являться недействительными.

Форма **set** данной команды используется для указания названия города.

Форма **delete** данной команды используется для удаления настройки города.

Форма **show** данной команды используется для отображения настройки города.

12.4.3 pki ca <имя> cn <общее_имя>

Указание общего имени (Common name), в качестве одного из атрибутов идентификатора УЦ.

Синтаксис

```
set pki ca <имя> cn <общее_имя>
delete pki ca <имя> cn
show pki ca <имя> cn
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        cn общее_имя
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

общее_имя

Обязательный. Общее имя (common name) удостоверяющего центра. В том случае если общее имя содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать общее имя, которое входит в идентификатор удостоверяющего центра. Идентификатор удостоверяющего центра представляет собой отличительное имя удостоверяющего центра в формате X.500, и состоит из набора иерархических атрибутов, в состав которых могут входить общее имя УЦ, адрес электронной почты, название организации и подразделения организации, атрибутов месторасположения таких как название страны, региона, города. Атрибут CN является обязательным атрибутом, указание его значения является обязательным при создании УЦ.

ПРИМЕЧАНИЕ Значения параметров УЦ, в том числе атрибутов идентификатора УЦ, не могут быть изменены после фиксации настройки. Для того чтобы изменить значения параметров УЦ, необходимо удалить настройку УЦ и создать ее заново, при этом для УЦ будет создана новая ключевая пара, соответственно с точки зрения системы, вновь созданный УЦ, даже при полном соответствии значений параметров, будет являться новым УЦ, отличным от предыдущего. Таким образом, сертификаты выпущенные до этого будут являться недействительными.

Форма **set** данной команды используется для указания общего имени удостоверяющего центра.

Форма **delete** данной команды используется для удаления настройки общего имени удостоверяющего центра.

Форма **show** данной команды используется для отображения настройки общего имени удостоверяющего центра.

12.4.4 pki ca <имя> country <страна>

Указание названия страны, в качестве одного из атрибутов идентификатора УЦ.

Синтаксис

```
set pki ca <имя> country <страна>
delete pki ca <имя> country
show pki ca <имя> country
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
```

```
    ca имя {
        country страна
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

страна

Двухбуквенный код страны.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать название страны, которое входит в идентификатор удостоверяющего центра. Идентификатор удостоверяющего центра представляет собой отличительное имя удостоверяющего центра в формате X.500, и состоит из набора иерархических атрибутов, в состав которых могут входить общее имя УЦ, адрес электронной почты, название организации и подразделения организации, атрибутов месторасположения таких как название страны, региона, города. Указание двухбуквенного кода страны не является обязательным.

ПРИМЕЧАНИЕ Значения параметров УЦ, в том числе атрибутов идентификатора УЦ, не могут быть изменены после фиксации настройки. Для того чтобы изменить значения параметров УЦ, необходимо удалить настройку УЦ и создать ее заново, при этом для УЦ будет создана новая ключевая пара, соответственно с точки зрения системы, вновь созданный УЦ, даже при полном соответствии значений параметров, будет являться новым УЦ, отличным от предыдущего. Таким образом, сертификаты выпущенные до этого будут являться недействительными.

Форма **set** данной команды используется для указания страны удостоверяющего центра.

Форма **delete** данной команды используется для удаления настройки страны удостоверяющего центра.

Форма **show** данной команды используется для отображения настройки страны удостоверяющего центра.

12.4.5 pki ca <имя> crldp <адрес>

Указание адреса точки распространения списка отзывов сертификатов УЦ.

Синтаксис

```
set pki ca <имя> crldp <адрес>
delete pki ca <имя> crldp
show pki ca <имя> crldp
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        crldp адрес
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

адрес

Множественный. Адрес точки распространения списка отзывов сертификатов (CRL Distribution Point). Можно определить несколько удостоверяющих центров, создав соответствующее количество узлов конфигурации.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать адрес точки распространения списка отзывов сертификатов (CRL distribution point). Точка распространения списка отзывов сертификатов содержит список отзыва сертификатов (CRL), подписанный определённым удостоверяющим центром (CA).

ПРИМЕЧАНИЕ Значения параметров УЦ, в том числе атрибутов идентификатора УЦ, не могут быть изменены после фиксации настройки. Для того чтобы изменить значения параметров УЦ, необходимо удалить настройку УЦ и создать ее заново, при этом для УЦ будет создана новая ключевая пара, соответственно с точки зрения системы, вновь созданный УЦ, даже при полном соответствии значений параметров, будет являться новым УЦ, отличным от предыдущего. Таким образом, сертификаты выпущенные до этого будут являться недействительными.

Форма **set** данной команды используется для указания адреса точки распространения списка отзывов сертификатов данного УЦ.

Форма **delete** данной команды используется для удаления адреса точки распространения списка отзывов сертификатов.

Форма **show** данной команды используется для отображения адреса точки распространения списка отзывов сертификатов.

12.4.6 pki ca <имя> email <email>

Указание адреса электронной почты, в качестве одного из атрибутов идентификатора УЦ.

Синтаксис

```
set pki ca <имя> email <email>
delete pki ca <имя> email
show pki ca <имя> email
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        email email
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

email

Адрес электронной почты.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать адрес электронной почты, который входит в идентификатор удостоверяющего центра. Идентификатор удостоверяющего центра представляет собой отличительное имя удостоверяющего центра в формате X.500, и состоит из набора иерархических атрибутов, в состав которых могут входить общее имя УЦ, адрес электронной почты, название организации и подразделения организации, атрибутов месторасположения таких как название страны, региона, города. Указание адреса электронной почты не является обязательным.

ПРИМЕЧАНИЕ Значения параметров УЦ, в том числе атрибутов идентификатора УЦ, не могут быть изменены после фиксации настройки. Для того чтобы изменить значения параметров УЦ, необходимо удалить настройку УЦ и создать ее заново, при этом для УЦ будет создана новая ключевая пара, соответственно с точки зрения системы, вновь созданный УЦ, даже при полном соответствии значений параметров, будет являться новым УЦ, отличным от предыдущего. Таким образом, сертификаты выпущенные до этого будут являться недействительными.

Форма **set** данной команды используется для указания адреса электронной почты.

Форма **delete** данной команды используется для удаления настройки адреса электронной почты.

Форма **show** данной команды используется для отображения настройки адреса электронной почты.

12.4.7 pki ca <имя> expiration <количество_дней>

Указание количества дней, в течение которого будет действителен сертификат УЦ.

Синтаксис

```
set pki ca <имя> expiration <количество_дней>
delete pki ca <имя> expiration
show pki ca <имя> expiration
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
   ca имя {
      expiration количество_дней
   }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

количество_дней

Количество дней, в течение которого сертификат удостоверяющего центра будет действителен. Сертификат удостоверяющего центра действителен с момента создания в течение указанного количества дней. По умолчанию сертификат удостоверяющего центра действителен в течение 1 года (365 дней). Этот параметр может принимать значение от 1 до 40000.

Значение по умолчанию

По умолчанию установлено значение 365.

Указания по использованию

Данная команда используется для указания периода действия сертификата удостоверяющего центра. Период действия сертификата удостоверяющего центра начинается с момента создания удостоверяющего центра. Сертификат является действительным в течение указанного количества дней. После истечения срока действия сертификата удостоверяющего центра сертификаты, выпущенные данным удостоверяющим центром, становятся недействительными.

ПРИМЕЧАНИЕ Значения параметров УЦ, в том числе атрибутов идентификатора УЦ, не могут быть изменены после фиксации настройки. Для того чтобы изменить значения параметров УЦ, необходимо удалить настройку УЦ и создать ее заново, при этом для УЦ будет создана новая ключевая пара, соответственно с точки зрения системы, вновь созданный УЦ, даже при полном соответствии значений параметров, будет являться новым УЦ, отличным от предыдущего. Таким образом, сертификаты выпущенные до этого будут являться недействительными.

Узел конфигурации **expiration** действителен только на этапе создания сертификата УЦ, на основе этого узла автоматически устанавливается дата окончания периода действия сертификата УЦ в качестве значения для узла **expires-on**. В дальнейшем для просмотра периода действия сертификата УЦ используется команда **show pki ca** <имя> **expires-on**.

Форма **set** данной команды используется для указания периода действия сертификата удостоверяющего центра.

Форма **delete** данной команды используется для удаления настройки периода действия сертификата удостоверяющего центра.

Форма **show** данной команды используется для отображения настройки периода действия сертификата удостоверяющего центра.

12.4.8 pki ca <имя> expires-on <окончание_периода_действия>

Указание даты окончания периода действия сертификата удостоверяющего центра.

Синтаксис

```
show pki ca <имя> expires-on
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        expires-on окончание_периода_действия
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

окончание_периода_действия

Дата и время окончания периода действия сертификата удостоверяющего центра. Значение для этого параметра создается автоматически при создании сертификата УЦ на основе значения, указанного при помощи команды **pki ca <имя> expiration <количество_дней>**. Изменение этого параметра невозможно.

Значение по умолчанию

Отсутствует.

Указания по использованию

Дата и время окончания периода действия сертификата удостоверяющего центра указывается автоматически на основе заданного периода действия сертификата УЦ. Период действия указывается при создании сертификата УЦ при помощи команды **pki ca <имя> expiration <количество_дней>**. Период действия начинается с момента создания удостоверяющего центра. После истечения срока действия сертификата удостоверяющего центра сертификаты, выпущенные данным удостоверяющим центром, становятся недействительными.

Форма **show** данной команды используется для отображения даты окончания периода действия сертификата удостоверяющего центра.

12.4.9 pki ca <имя> key-curve <название_кривой>

Указание названия ECDSA-кривой.

Синтаксис

```
set pki ca <имя> key-curve <название_кривой>
delete pki ca <имя> key-curve
show pki ca <имя> key-curve
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        key-curve название_кривой
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

название_кривой

Название эллиптической кривой в терминологии openssl. Для использования доступны все типы эллиптических кривых, поддерживаемые актуальной версией openssl для алгоритма ECDSA.

Значение по умолчанию

По умолчанию используется эллиптическая кривая **prime256v1**.

Указания по использованию

Данная команда позволяет указать тип эллиптической кривой, используемой для сертификатов с алгоритмом ECDSA. Размер ключа для каждой эллиптической кривой вычисляется автоматически и задания не требует.

Форма **set** данной команды используется для указания длины используемого ключа.

Форма **delete** данной команды используется для удаления настройки длины используемого ключа.

Форма **show** данной команды используется для отображения настройки длины используемого ключа.

12.4.10 pki ca <имя> key-size <длина_ключа>

Указание длины используемого ключа.

Синтаксис

```
set pki ca <имя> key-size <длина_ключа>
delete pki ca <имя> key-size
show pki ca <имя> key-size
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        key-size длина_ключа
    }
```

```
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

длина_ключа

Длина используемого ключа в битах. Допустимые значения представлены в таблице ниже.

Таблица 52 – Значения длины ключа в зависимости от используемого алгоритма.

Значение	Описание
256	Если используется алгоритм ГОСТ 34.10-2001 или алгоритм ГОСТ 34.10-2012
512	Если используется алгоритм ГОСТ 34.10-2012
1024-8192	Если используется алгоритм RSA

Значение по умолчанию

При использовании алгоритмов ГОСТ 34.10-2001 и ГОСТ 34.10-2012 устанавливается длина ключа 256 бит.

При использовании алгоритма RSA устанавливается длина ключа 1024 бит.

При использовании алгоритма ECDSA длинна ключа вычисляется автоматически для каждой эллиптической кривой.

Указания по использованию

Данная команда позволяет указать длину используемого ключа. Допустимые значения зависит от типа используемого криптографического алгоритма: при использовании ГОСТ 34.10-2001 допустимая длина ключа 256 бит, при использовании ГОСТ 34.10-2012 допустимая длина ключа 256 и 512 бит, при использовании RSA допустимая длина ключа должна лежать в диапазоне от 1024 до 8192 бит.

Если указан алгоритм ECDSA и заданный размер ключа отличается от вычисленного автоматически, такая конфигурация применена не будет с соответствующим сообщением об ошибке.

Форма **set** данной команды используется для указания длины используемого ключа.

Форма **delete** данной команды используется для удаления настройки длины используемого ключа.

Форма **show** данной команды используется для отображения настройки длины используемого ключа.

12.4.11 pki ca <имя> key-type <тип_ключа>

Указание криптографического алгоритма, используемого для защиты данных.

Синтаксис

```
set pki ca <имя> key-type <тип_ключа>
delete pki ca <имя> key-type
show pki ca <имя> key-type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca текст {
        key-type тип_ключа
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

тип_ключа

Используемый криптографический алгоритм. Допустимые значения представлены в таблице ниже.

Таблица 53 – Допустимые криптографические алгоритмы.

Значение	Описание
gost2001	Алгоритм ГОСТ 34.10-2001
gost2012	Алгоритм ГОСТ 34.10-2012
rsa	Алгоритм RSA

Значение по умолчанию

По умолчанию установлено значение **gost2012**.

Указания по использованию

Данная команда позволяет указать тип используемого для защиты данных криптографического алгоритма. По умолчанию используется алгоритм ГОСТ 34.10-2012.

ПРИМЕЧАНИЕ Значения параметров УЦ, в том числе атрибутов идентификатора УЦ, не могут быть изменены после фиксации настройки. Для того чтобы изменить значения параметров УЦ, необходимо удалить настройку УЦ и создать ее заново, при этом для УЦ будет создана новая ключевая пара, соответственно с точки зрения системы, вновь созданный УЦ, даже при полном соответствии значений параметров, будет являться новым УЦ, отличным от предыдущего. Таким образом, сертификаты выпущенные до этого будут являться недействительными.

Форма **set** данной команды используется для указания типа используемого криптографического алгоритма.

Форма **delete** данной команды используется для удаления настройки типа используемого криптографического алгоритма.

Форма **show** данной команды используется для отображения настройки типа используемого криптографического алгоритма.

12.4.12 pki ca <имя> last-update <последнее_обновление_CRL>

Дата и время последнего обновления CRL для данного УЦ.

Синтаксис

show pki ca <имя> last-update

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        last-update последнее_обновление_CRL
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

последнее_обновление_CRL

Дата и время последнего обновления списка отзыва сертификатов.

Значение по умолчанию

Отсутствует.

Указания по использованию

На этапе создания УЦ последним обновлением CRL считается дата и время этого УЦ. В последующей эксплуатации – это значение может изменяться после генерации нового CRL либо после отзыва конечного сертификата. Изменение этого параметра вручную через систему конфигурации невозможно.

Форма **show** данной команды используется для отображения даты и времени последнего обновления CRL.

12.4.13 pki ca <имя> next-update <окончание_срока_действия_CRL>

Указание даты и времени окончания периода действия CRL для данного удостоверяющего центра.

Синтаксис

show pki ca <имя> expires-on

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        expires-on окончание_периода_действия
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

окончание_периода_действия

Дата и время окончания периода действия CRL для данного удостоверяющего центра. Значение для этого параметра создается автоматически при создании сертификата УЦ на основе значения, указанного при помощи команды **pki ca <имя> expiration <количество_дней>**. Изменение этого параметра невозможно.

Значение по умолчанию

Отсутствует.

Указания по использованию

Дата и время окончания периода действия CRL для данного удостоверяющего центра.

- При генерации УЦ на Numa Edge, данное значение задается автоматически на основе значения, указанного при помощи команды **pki ca <имя> expiration <количество_дней>**, т.е равно сроку действия самого УЦ.
- При импорте CRL для стороннего УЦ, устанавливается указанное им значение. Обновление CRL осуществляется с помощью команды **pki update-crl <название_УЦ>.**

После истечения срока действия CRL сертификаты перестают проходить проверку подлинности и считаются недействительными.

Форма **show** данной команды используется для отображения даты и времени окончания периода действия CRL для данного удостоверяющего центра.

12.4.14 pki ca <имя> organization <организация>

Указание названия организации, в качестве одного из атрибутов идентификатора УЦ.

Синтаксис

```
set pki ca <имя> organization <организация>
delete pki ca <имя> organization
show pki ca <имя> organization
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        organisation организация
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

организация

Название организации. В том случае если название организации содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать название организации, которое входит в идентификатор удостоверяющего центра. Идентификатор удостоверяющего центра представляет собой отличительное имя удостоверяющего центра в формате X.500, и состоит из набора иерархических атрибутов, в состав которых могут входить общее имя УЦ, адрес электронной почты, название организации и подразделения организации, атрибутов месторасположения таких как название страны, региона, города. Указание названия организации не является обязательным.

ПРИМЕЧАНИЕ Значения параметров УЦ, в том числе атрибутов идентификатора УЦ, не могут быть изменены после фиксации настройки. Для того чтобы изменить значения параметров УЦ, необходимо удалить настройку УЦ и создать ее заново, при этом для УЦ будет создана новая ключевая пара, соответственно с точки зрения системы, вновь созданный УЦ, даже при полном соответствии значений параметров, будет являться новым УЦ, отличным от предыдущего. Таким образом, сертификаты выпущенные до этого будут являться недействительными.

Форма **set** данной команды используется для указания названия организации.

Форма **delete** данной команды используется для удаления настройки названия организации.

Форма **show** данной команды используется для отображения настройки названия организации.

12.4.15 pki ca <имя> organization-unit <подразделение>

Указание названия подразделения организации, в качестве одного из атрибутов идентификатора УЦ.

Синтаксис

```
set pki ca <имя> organization-unit <подразделение>
delete pki ca <имя> organization-unit
show pki ca <имя> organization-unit
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        organisation-unit подразделение
```

```
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

подразделение

Название подразделения организации. В том случае если название подразделения организации содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать название подразделения организации, которое входит в идентификатор удостоверяющего центра. Идентификатор удостоверяющего центра представляет собой отличительное имя удостоверяющего центра в формате X.500, и состоит из набора иерархических атрибутов, в состав которых могут входить общее имя УЦ, адрес электронной почты, название организации и подразделения организации, атрибутов месторасположения таких как название страны, региона, города. Указание названия подразделения организации не является обязательным.

ПРИМЕЧАНИЕ Значения параметров УЦ, в том числе атрибутов идентификатора УЦ, не могут быть изменены после фиксации настройки. Для того чтобы изменить значения параметров УЦ, необходимо удалить настройку УЦ и создать ее заново, при этом для УЦ будет создана новая ключевая пара, соответственно с точки зрения системы, вновь созданный УЦ, даже при полном соответствии значений параметров, будет являться новым УЦ, отличным от предыдущего. Таким образом, сертификаты выпущенные до этого будут являться недействительными.

Форма **set** данной команды используется для указания названия подразделения организации.

Форма **delete** данной команды используется для удаления настройки названия подразделения организации.

Форма **show** данной команды используется для отображения настройки названия подразделения организации.

12.4.16 pki ca <имя> province <регион>

Указание названия региона, в качестве одного из атрибутов идентификатора УЦ.

Синтаксис

```
set pki ca <имя> province <регион>
delete pki ca <имя> province
show pki ca <имя> province
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        province регион
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

регион

Название региона. В том случае если название региона содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать название региона, которое входит в идентификатор удостоверяющего центра. Идентификатор удостоверяющего центра представляет собой отличительное имя удостоверяющего центра в формате X.500, и состоит из набора иерархических атрибутов, в состав которых могут входить общее имя УЦ, адрес электронной почты, название организации и подразделения организации, атрибутов месторасположения таких как название страны, региона, города. Указание названия региона не является обязательным.

ПРИМЕЧАНИЕ Значения параметров УЦ, в том числе атрибутов идентификатора УЦ, не могут быть изменены после фиксации настройки. Для того чтобы изменить значения параметров УЦ, необходимо удалить настройку УЦ и создать ее заново, при этом для УЦ будет создана новая ключевая пара, соответственно с точки зрения системы, вновь созданный УЦ, даже при полном соответствии значений параметров, будет являться новым УЦ, отличным от предыдущего. Таким образом, сертификаты выпущенные до этого будут являться недействительными.

Форма **set** данной команды используется для указания названия региона.

Форма **delete** данной команды используется для удаления настройки названия региона.

Форма **show** данной команды используется для отображения настройки названия региона.

12.4.17 pki ca <имя> certificate <имя_сертификата>

Определение сертификата субъекта, подписанного указанным удостоверяющим центром.

Синтаксис

```
set pki ca <имя> certificate <имя_сертификата>
delete pki ca <имя> certificate
show pki ca <имя> certificate
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        certificate имя_сертификата {
        }
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

имя_сертификата

Название узла конфигурации сертификата.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для создания сертификата субъекта, который будет заверен электронной цифровой подписью указанного удостоверяющего центра.

Непосредственное использование открытых ключей требует дополнительной их защиты и идентификации для определения связи с секретным ключом. Электронный сертификат представляет собой цифровой документ, который связывает открытый ключ с его владельцем, субъектом сертификата. Для заверения электронного сертификата используется электронная цифровая подпись удостоверяющего центра (УЦ). УЦ включает свое имя в каждый выпущенный им сертификат и подписывает их при помощи собственного секретного ключа. Для проверки подлинности сертификата субъекта используется сертификат удостоверяющего центра, включающий открытый ключ УЦ. Под субъектом понимается сторона, контролирующая секретный ключ, соответствующий открытому ключу, указанному в сертификате.

Форма **set** данной команды используется для создания сертификата субъекта.

Форма **delete** данной команды используется для удаления настройки сертификата.

Форма **show** данной команды используется для отображения настройки сертификата.

12.4.18 pki ca <имя> certificate <имя_сертификата> alternative-name email <email>

Указание адреса электронной почты в качестве атрибута расширения альтернативного имени субъекта.

Синтаксис

```
set pki ca <имя> certificate <имя_сертификата> alternative-name email <email>
delete pki ca <имя> certificate <имя_сертификата> alternative-name email
show pki ca <имя> certificate <имя_сертификата> alternative-name email
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        certificate имя_сертификата {
            alternative-name {
                email email
            }
        }
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

имя_сертификата

Название узла конфигурации сертификата.

email

Адрес электронной почты.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать адрес электронной почты в качестве атрибута расширения X.509v3 альтернативного имени субъекта сертификата (Subject Alternative Name). Под субъектом понимается сторона, контролирующая секретный ключ, соответствующий открытому ключу, указанному в сертификате. Использование данного расширения позволяет указать дополнительные домены в рамках одного сертификата.

Указание атрибутов данного расширения не является обязательным.

ПРИМЕЧАНИЕ Значения атрибутов идентификатора субъекта сертификата, не могут быть изменены после фиксации настройки. При необходимости их изменения необходимо удалить настройку сертификата и создать заново.

Форма **set** данной команды используется для указания адреса электронной почты расширения альтернативного имени субъекта.

Форма **delete** данной команды используется для удаления адреса электронной почты расширения альтернативного имени субъекта.

Форма **show** данной команды используется для отображения адреса электронной почты расширения альтернативного имени субъекта.

12.4.19 pki ca <имя> certificate <имя_сертификата> alternative-name idn <доменное_имя>

Указание доменного имени в качестве атрибута расширения альтернативного имени субъекта.

Синтаксис

```
set pki ca <имя> certificate <имя_сертификата> alternative-name idn <доменное_имя>
delete pki ca <имя> certificate <имя_сертификата> alternative-name idn
show pki ca <имя> certificate <имя_сертификата> alternative-name idn
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        certificate имя_сертификата {
            alternative-name {
                idn доменное имя
            }
        }
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

имя_сертификата

Название узла конфигурации сертификата.

idn

Международное доменное имя субъекта.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать доменное имя в качестве атрибута расширения X.509v3 альтернативного имени субъекта сертификата (Subject Alternative Name). Под субъектом понимается сторона, контролирующая секретный ключ, соответствующий открытому ключу, указанному в сертификате. Использование данного расширения позволяет указать дополнительные домены в рамках одного сертификата.

Указание атрибутов данного расширения не является обязательным.

ПРИМЕЧАНИЕ Значения атрибутов идентификатора субъекта сертификата, не могут быть изменены после фиксации настройки. При необходимости их изменения необходимо удалить настройку сертификата и создать заново.

Форма **set** данной команды используется для указания доменного имени расширения альтернативного имени субъекта.

Форма **delete** данной команды используется для удаления доменного имени расширения альтернативного имени субъекта.

Форма **show** данной команды используется для отображения доменного имени расширения альтернативного имени субъекта.

12.4.20 pki ca <имя> certificate <имя_сертификата> alternative-name ip-address <ip-адрес>

Указание IP-адреса в качестве атрибута расширения альтернативного имени субъекта.

Синтаксис

```
set pki ca <имя> certificate <имя_сертификата> alternative-name ip-address <ip-адрес>
delete pki ca <имя> certificate <имя_сертификата> alternative-name ip-address
show pki ca <имя> certificate <имя_сертификата> alternative-name ip-address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        certificate имя_сертификата {
            alternative-name {
                ip-address ip-адрес
            }
        }
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

имя_сертификата

Название узла конфигурации сертификата.

ip-адрес

IP адрес субъекта. Допустимые значения представлены в таблице ниже.

Таблица 54 – Формат IP-адреса расширения альтернативного имени субъекта.

Значение	Описание
<x.x.x.x>	IPv4 адрес
<h:h:h:h:h:h:h:h>	IPv6 адрес

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать IP адрес в качестве атрибута расширения X.509v3 альтернативного имени субъекта сертификата (Subject Alternative Name). Под субъектом понимается сторона, контролирующая секретный ключ, соответствующий открытому ключу, указанному в сертификате. Использование данного расширения позволяет указать дополнительные домены в рамках одного сертификата.

Указание атрибутов данного расширения не является обязательным.

ПРИМЕЧАНИЕ Значения атрибутов идентификатора субъекта сертификата, не могут быть изменены после фиксации настройки. При необходимости их изменения необходимо удалить настройку сертификата и создать заново.

Форма **set** данной команды используется для указания IP-адреса расширения альтернативного имени субъекта.

Форма **delete** данной команды используется для удаления IP-адреса расширения альтернативного имени субъекта.

Форма **show** данной команды используется для отображения IP-адреса расширения альтернативного имени субъекта.

12.4.21 pki ca <имя> certificate <имя_сертификата> city <город>

Указание названия города, в качестве одного из атрибутов идентификатора субъекта сертификата.

Синтаксис

```
set pki ca <имя> certificate <имя_сертификата> city <город>
delete pki ca <имя> certificate <имя_сертификата> city
show pki ca <имя> certificate <имя_сертификата> city
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        certificate имя_сертификата {
            city город
        }
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

имя_сертификата

Название узла конфигурации сертификата.

город

Название города. В том случае если название содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать название города, которое входит в идентификатор субъекта сертификата. Под субъектом понимается сторона, контролирующая секретный ключ, соответствующий открытому ключу, указанному в сертификате. Идентификатор субъекта представляет собой отличительное имя субъекта в формате X.500, и состоит из набора иерархических атрибутов, в состав которых могут входить общее имя, адрес электронной почты, название организации и подразделения организации, атрибутов месторасположения таких как название страны, региона, города.

Указание названия города не является обязательным.

ПРИМЕЧАНИЕ Значения атрибутов идентификатора субъекта сертификата, не могут быть изменены после фиксации настройки. При необходимости их изменения необходимо удалить настройку сертификата и создать заново.

Форма **set** данной команды используется для указания названия города.

Форма **delete** данной команды используется для удаления настройки города.

Форма **show** данной команды используется для отображения настройки города.

12.4.22 pki ca <имя> certificate <имя_сертификата> cn <общее_имя>

Указание общего имени, в качестве одного из атрибутов идентификатора субъекта.

Синтаксис

```
set pki ca <имя> certificate <имя_сертификата> cn <общее_имя>
delete pki ca <имя> certificate <имя_сертификата> cn
show pki ca <имя> certificate <имя_сертификата> cn
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        certificate имя_сертификата {
            cn общее_имя
        }
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

имя_сертификата

Название узла конфигурации сертификата.

общее_имя

Обязательный. Общее имя (common name) субъекта сертификата. В том случае если общее имя содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать общее имя (common name), которое входит в идентификатор субъекта сертификата. Под субъектом понимается сторона, контролирующая секретный ключ, соответствующий открытому ключу, указанному в сертификате. Идентификатор субъекта представляет собой отличительное имя субъекта в формате X.500, и состоит из набора иерархических атрибутов, в состав которых могут входить общее имя, адрес электронной почты, название организации и подразделения организации, атрибутов месторасположения таких как название страны, региона, города.

Указание общего имени субъекта сертификата является обязательным.

ПРИМЕЧАНИЕ Значения атрибутов идентификатора субъекта сертификата, не могут быть изменены после фиксации настройки. При необходимости их изменения необходимо удалить настройку сертификата и создать заново.

Форма **set** данной команды используется для указания общего имени субъекта сертификата.

Форма **delete** данной команды используется для удаления настройки общего имени субъекта сертификата.

Форма **show** данной команды используется для отображения настройки общего имени субъекта сертификата.

12.4.23 pki ca <имя> certificate <имя_сертификата> country <страна>

Указание названия страны, в качестве одного из атрибутов идентификатора субъекта сертификата.

Синтаксис

```
set pki ca <имя> certificate <имя_сертификата> country <страна>
delete pki ca <имя> certificate <имя_сертификата> country
show pki ca <имя> certificate <имя_сертификата> country
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        certificate имя_сертификата {
            country страна
        }
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

имя_сертификата

Название узла конфигурации сертификата.

страна

Двухбуквенный код страны.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать двухбуквенный код страны, который входит в идентификатор субъекта сертификата. Под субъектом понимается сторона, контролирующая секретный ключ, соответствующий открытому ключу, указанному в сертификате. Идентификатор субъекта представляет собой отличительное имя субъекта в формате X.500, и состоит из набора иерархических атрибутов, в состав которых могут входить общее имя, адрес электронной почты, название организации и подразделения организации, атрибутов месторасположения таких как название страны, региона, города.

Указание страны не является обязательным.

ПРИМЕЧАНИЕ Значения атрибутов идентификатора субъекта сертификата, не могут быть изменены после фиксации настройки. При необходимости их изменения необходимо удалить настройку сертификата и создать заново.

Форма **set** данной команды используется для указания кода страны.

Форма **delete** данной команды используется для удаления настройки страны.

Форма **show** данной команды используется для отображения настройки страны.

12.4.24 pki ca <имя> certificate <имя_сертификата> expiration <количество_дней>

Указание количества дней, в течение которого будет действителен указанный сертификат.

Синтаксис

```
set pki ca <имя> certificate <имя_сертификата> expiration <количество_дней>
delete pki ca <имя> certificate <имя_сертификата> expiration
show pki ca <имя> certificate <имя_сертификата> expiration
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        certificate имя_сертификата {
            expiration количество_дней
        }
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

имя_сертификата

Название узла конфигурации сертификата.

количество_дней

Количество дней, в течение которого сертификат будет действителен. Сертификат действителен с момента создания в течение указанного количества дней. По умолчанию сертификат субъекта действителен в течение 1 года (365 дней).

Значение по умолчанию

По умолчанию сертификат субъекта действителен в течение 1 года (365 дней).

Указания по использованию

Данная команда используется для указания периода действия сертификата субъекта. Под субъектом понимается сторона, контролирующая секретный ключ, соответствующий открытому ключу, указанному в сертификате. Период действия сертификата начинается с момента создания сертификата (при фиксации настройки сертификата). Сертификат является действительным в течение указанного количества дней. После истечения срока действия сертификата он становится недействительным.

Узел конфигурации **expiration** действителен только на этапе создания сертификата, на основе этого узла автоматически устанавливается дата окончания периода действия сертификата в качестве значения для узла **expires-on**. В дальнейшем для просмотра периода действия сертификата используется команда **show pki ca** имя **certificate** имя_сертификата **expires-on**.

Форма **set** данной команды используется для указания периода действия сертификата субъекта.

Форма **delete** данной команды используется для удаления настройки периода действия сертификата субъекта.

Форма **show** данной команды используется для отображения настройки периода действия сертификата субъекта.

12.4.25 pki ca <имя> certificate <имя_сертификата> expires-on <окончание_периода_действия>

Указание даты и времени окончания периода действия данного сертификата.

Синтаксис

```
show pki ca <имя> certificate <имя_сертификата> expires-on
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
  ca имя {
     certificate имя_сертификата {
        expires-on окончание_периода_действия
      }
   }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

имя_сертификата

Название узла конфигурации сертификата.

окончание_периода_действия

Дата и время окончания периода действия сертификата. Значение для этого параметра создается автоматически при создании сертификата на основе значения, указанного при помощи команды **pki ca <имя> certificate <имя_сертификата> expiration <количество_дней>**. Изменение этого параметра невозможно.

Значение по умолчанию

Отсутствует.

Указания по использованию

Дата и время окончания периода действия сертификата субъекта указывается автоматически на основе заданного периода действия сертификата. Период действия указывается при создании сертификата при помощи команды **pki ca <имя> certificate <имя_сертификата> expiration <количество_дней>**. Период действия начинается с момента создания сертификата.

Форма **show** данной команды используется для отображения даты и времени окончания периода действия сертификата субъекта.

12.4.26 pki ca <имя> certificate <имя_сертификата> organization <подразделение>

Указание названия организации, в качестве одного из атрибутов идентификатора субъекта.

Синтаксис

```
set pki ca <имя> certificate <имя_сертификата> organization <организация>
delete pki ca <имя> certificate <имя_сертификата> organization
show pki ca <имя> certificate <имя_сертификата> organization
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
   ca имя {
      certificate имя_сертификата {
         organization организация
      }
   }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

имя_сертификата

Название узла конфигурации сертификата.

организация

Название организации. В том случае если название организации содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать название организации, которое входит в идентификатор субъекта сертификата. Под субъектом понимается сторона, контролирующая секретный ключ, соответствующий открытому ключу, указанному в сертификате. Идентификатор субъекта представляет собой отличительное имя субъекта в формате X.500, и состоит из набора иерархических атрибутов, в состав которых могут входить общее имя, адрес электронной почты, название организации и подразделения организации, атрибутов месторасположения таких как название страны, региона, города.

Указание организации не является обязательным.

ПРИМЕЧАНИЕ Значения атрибутов идентификатора субъекта сертификата, не могут быть изменены после фиксации настройки. При необходимости их изменения необходимо удалить настройку сертификата и создать заново.

Форма **set** данной команды используется для указания организации.

Форма **delete** данной команды используется для удаления настройки организации.

Форма **show** данной команды используется для отображения настройки организации.

12.4.27 pki ca <имя> certificate <имя_сертификата> organization-unit <подразделение>

Указание названия подразделения, в качестве одного из атрибутов идентификатора субъекта.

Синтаксис

```
set pki ca <имя> certificate <имя_сертификата> organization-unit <подразделение>
delete pki ca <имя> certificate <имя_сертификата> organization-unit
show pki ca <имя> certificate <имя_сертификата> organization-unit
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        certificate имя_сертификата {
            organization-unit подразделение
        }
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

имя_сертификата

Название узла конфигурации сертификата.

подразделение

Название подразделения организации. В том случае если название подразделения организации содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать название подразделения организации, которое входит в идентификатор субъекта сертификата. Под субъектом понимается сторона, контролирующая секретный ключ, соответствующий открытому ключу, указанному в сертификате. Идентификатор субъекта представляет собой отличительное имя субъекта в формате X.500, и состоит из набора иерархических атрибутов, в состав которых могут входить общее имя, адрес электронной почты, название организации и подразделения организации, атрибутов месторасположения таких как название страны, региона, города.

Указание подразделения организации не является обязательным.

ПРИМЕЧАНИЕ Значения атрибутов идентификатора субъекта сертификата, не могут быть изменены после фиксации настройки. При необходимости их изменения необходимо удалить настройку сертификата и создать заново.

Форма **set** данной команды используется для указания подразделения организации.

Форма **delete** данной команды используется для удаления настройки подразделения организации.

Форма **show** данной команды используется для отображения настройки подразделения организации.

12.4.28 pki ca <имя> certificate <имя_сертификата> email <email>

Указание адреса электронной почты, в качестве одного из атрибутов идентификатора субъекта.

Синтаксис

```
set pki ca <имя> certificate <имя_сертификата> email <email>
delete pki ca <имя> certificate <имя_сертификата> email
show pki ca <имя> certificate <имя_сертификата> email
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        certificate имя_сертификата {
            email email
        }
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

имя_сертификата

Название узла конфигурации сертификата.

email

Адрес электронной почты.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать адрес электронной почты, который входит в идентификатор субъекта сертификата. Под субъектом понимается сторона, контролирующая секретный ключ, соответствующий открытому ключу, указанному в сертификате. Идентификатор субъекта представляет собой отличительное имя субъекта в формате X.500, и состоит из набора иерархических атрибутов, в состав которых могут входить общее имя, адрес электронной почты, название организации и подразделения организации, атрибутов месторасположения таких как название страны, региона, города.

Указание адреса электронной почты субъекта сертификата не является обязательным.

ПРИМЕЧАНИЕ Значения атрибутов идентификатора субъекта сертификата, не могут быть изменены после фиксации настройки. При необходимости их изменения необходимо удалить настройку сертификата и создать заново.

Форма **set** данной команды используется для указания адреса электронной почты субъекта сертификата.

Форма **delete** данной команды используется для удаления настройки адреса электронной почты субъекта сертификата.

Форма **show** данной команды используется для отображения настройки адреса электронной почты субъекта сертификата.

12.4.29 pki ca <имя> certificate <имя_сертификата> province <регион>

Указание адреса региона, в качестве одного из атрибутов идентификатора субъекта.

Синтаксис

```
set pki ca <имя> certificate <имя_сертификата> province <регион>
delete pki ca <имя> certificate <имя_сертификата> province
show pki ca <имя> certificate <имя_сертификата> province
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
   ca имя {
      certificate имя_сертификата {
         province регион
      }
   }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

имя_сертификата

Название узла конфигурации сертификата.

регион

Название региона. В том случае если название региона содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать регион, который входит в идентификатор субъекта сертификата. Под субъектом понимается сторона, контролирующая секретный ключ, соответствующий открытому ключу, указанному в сертификате. Идентификатор субъекта представляет собой отличительное имя субъекта в формате X.500, и состоит из набора иерархических атрибутов, в состав которых могут входить общее имя, адрес электронной почты, название организации и подразделения организации, атрибутов месторасположения таких как название страны, региона, города.

Указание региона для субъекта сертификата не является обязательным.

ПРИМЕЧАНИЕ Значения атрибутов идентификатора субъекта сертификата, не могут быть изменены после фиксации настройки. При необходимости их изменения необходимо удалить настройку сертификата и создать заново.

Форма **set** данной команды используется для указания региона.

Форма **delete** данной команды используется для удаления настройки региона.

Форма **show** данной команды используется для отображения настройки региона.

12.4.30 pki ca <имя> certificate <имя_сертификата> usage <сторона> <состояние>

Указание ограничений по использованию сертификата в расширении X509v3.

Синтаксис

```
set pki ca <имя> certificate <имя_сертификата> usage <сторона> <состояние>
delete pki ca <имя> certificate <имя_сертификата> usage [<сторона>]
```

```
show pki ca <имя> certificate <имя_сертификата> usage [<сторона>]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
pki {
    ca имя {
        certificate имя_сертификата {
            usage {
                сторона состояние
            }
        }
    }
}
```

Параметры

имя

Название узла конфигурации удостоверяющего центра.

имя_сертификата

Название узла конфигурации сертификата.

сторона

Сторона, на которой используется TLS. Допустимые значения представлены в таблице ниже.

Таблица 55 – Возможные значения параметра "сторона"

Значение	Описание
client	Использование сертификата для аутентификации клиента по протоколу TLS.
server	Использование сертификата для аутентификации сервера по протоколу TLS.

состояние

Указывает возможность использование данного сертификата для выбранной стороны. Допустимые значения представлены в таблице ниже.

Таблица 56 – Состояния для сторон

Значение	Описание
true	Разрешается использовать сертификат для указанной стороны
false	Запрещается использовать сертификат для указанной стороны

Значение по умолчанию

Отсутствует

Указания по использованию

Данная команда позволяет установить ограничения по использованию для сертификата, используемого соединении TLS на стороне сервера или клиента.

Если ветка usage отсутствует, или если параметры **client** и **server** имеют значение **false**, то запись ограничивающих дополнений «область применения ключа» (KeyUsage) и «расширенная область применения ключа» (extendedKeyUsage) расширения X509v3 в указанный сертификат не производится.

При установке любого из параметров в состояние true, для полей KeyUsage и extendedKeyUsage устанавливается бит critical, означающий, что данное поле должно быть обработано, а в случае невозможности обработки - сертификат должен быть отклонен. Таким образом ПО, работающее с сертификатами - должно обрабатывать указанные биты.

При установке параметра client true значение поля extendedKeyUsage устанавливается в TLS Web Client Authentication.

При установке параметра server true значение поля extendedKeyUsage устанавливается в TLS Web Server Authentication.

Согласно RFC 5280 при установке значения TLS Web Client Authentication или TLS Web Server Authentication могут быть установлены следующие биты KeyUsage:

- digitalSignature - используется для проверки цифровых подписей;
- keyAgreement - используется для согласования ключевой информации, например при использовании обмена методом Диффи-Хеллмана;
- keyEncipherment - используется для ассиметричного шифрования других криптографических объектов, например закрытого ключа при обмене ключевой информацией.

Таким образом, система Numa Edge для обеспечения совместимости с различными реализациями УЦ устанавливает следующие значения расширений X509v3:

Если параметр **client** имеет значение **true**, то в указанный сертификат дописываются два ограничивающих дополнения:

- область применения ключа (KeyUsage) с битами critical, digitalSignature, keyAgreement;
- расширенная область применения ключа (extendedKeyUsage) с битами critical, TLS Web Client Authentication.

Если параметр **server** имеет значение **true**, то в указанный сертификат дописываются два ограничивающих дополнения:

- область применения ключа (KeyUsage) с битами critical, digitalSignature, keyEncipherment, keyAgreement;
- расширенная область применения ключа (extendedKeyUsage) с битами critical, TLS Web Client Authentication.

Если параметры **client** и **server** имеют значение **true**, то в этом случае в указанный сертификат дописываются два ограничивающих дополнения:

- область применения ключа (KeyUsage) с битами critical, digitalSignature, keyEncipherment, keyAgreement;
- расширенная область применения ключа (extendedKeyUsage) с битами critical, clientAuth, TLS Web Client Authentication, TLS Web Server Authentication.

Форма **set** данной команды используется для разрешения или запрета использования сертификата в качестве клиента или сервера за счет расширений X509v3.

Форма **delete** данной команды используется для восстановления значения по умолчанию.

Форма **show** данной команды используется для отображения установленного значения.

12.4.31 pki export ca <имя> crl <формат>

Экспорт файла со списком отозванных сертификатов в указанном формате.

Синтаксис

```
pki export ca <имя> crl <формат> [to <имя_файла>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя

Название узла конфигурации удостоверяющего центра.

формат

Формат списка отозванных сертификатов. Допустимые значения представлены в таблице ниже.

Таблица 57 – Допустимые форматы списка отозванных сертификатов

Значение	Описание
der	Список отозванных сертификатов в формате DER
pem	Список отозванных сертификатов в формате PEM

имя_файла

Имя файла, содержащего список отозванных сертификатов и его местоположение.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет экспортировать список отозванных сертификатов в формате DER или PEM. По умолчанию экспорт производится на подключенный флэш-накопитель. При выполнении данной команды к устройству должен быть подключен флэш-накопитель. Монтирование и размонтирование флэш-накопителя осуществляется автоматически. Экспортируемый файл будет помещен в корневую директорию флэш-накопителя.

При указании параметра «**to**» производится экспорт по указанному адресу, который может быть локальным или находиться на сервере TFTP, FTP или SCP.

В приведенной ниже таблице показан синтаксис указания файла для различных местоположений файла.

Таблица 58 – Допустимые форматы указания месторасположения выгружаемого списка отозванных сертификатов.

Местоположение	Способ указания
Абсолютный путь	Используется стандартный способ указания файла в UNIX.
Относительный путь	Указывается имя файла с путем относительно каталога конфигурации по умолчанию.
Сервер FTP	Используется следующий синтаксис для имя_файла: *ftp://пользователь@узел/файл_конфигурации* где *пользователь* – это имя пользователя на узле, *узел* – это имя узла или IP-адрес сервера FTP, а *файл_конфигурации*– это файл конфигурации, включая путь. Если *пользователь* не указан, будет выдан запрос на его ввод. Если аутентификация производится по паролю, далее будет запрошен пароль.
Сервер SCP	Используется следующий синтаксис для *имя_файла*: *scp://пользователь@узел/файл_конфигурации*, где *пользователь* – это имя пользователя на узле, *узел* это имя узла или IP-адрес сервера SCP, а *файл_конфигурации* – это файл конфигурации, включая путь. Если *пользователь* не указан, будет выдан запрос на его ввод. Если аутентификация производится по паролю, далее будет запрошен пароль.
Сервер TFTP	Используется следующий синтаксис для имя_файла: *tftp://узел/файл_конфигурации,* где *узел* – это имя узла или IP-адрес сервера TFTP, а *файл_конфигурации* – это файл конфигурации, включая путь относительно корневого каталога TFTP.

12.4.32 pki export certificate <имя_сертификата>

Экспорт сертификата субъекта, ключевой пары субъекта, сертификата УЦ, списка отозванных сертификатов.

Синтаксис

```
pki export certificate <имя_сертификата> [to <имя_файла>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_сертификата

Имя сертификата, который требуется экспортировать.

имя_файла

Имя архива, содержащего сертификат субъекта, ключевую пару субъекта, сертификат УЦ, список отозванных сертификатов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет экспортировать сертификат субъекта, сертификат УЦ, секретный ключ субъекта, а также список отозванных сертификатов. По умолчанию экспорт производится на подключенный флэш-накопитель. При выполнении данной команды к устройству должен быть подключен флэш-накопитель. Монтирование и размонтирование флэш-накопителя осуществляется автоматически. Экспортируемые файлы будут помещены в корневую директорию флэш-накопителя. К экспортируемым файлам относятся: сертификат удостоверяющего центра, сертификат клиента, подписанный указанным удостоверяющим центром, секретный ключ клиента и файл, содержащий список отозванных сертификатов.

Если в качестве объекта для экспорта указывается сертификат УЦ, а не сертификат субъекта, то список отозванных сертификатов и закрытый ключ УЦ не экспортируются, т.е. производится экспорт только сертификата УЦ.

При указании параметра «**to**» производится экспорт в архив формата tar.gz по указанному адресу, который может быть локальным или находиться на сервере TFTP, FTP или SCP.

В приведенной ниже таблице показан синтаксис указания файла для различных местоположений файла.

Таблица 59 – Способы указания местоположения для экспорта сертификата

Местоположение	Способ указания
Путь в локальной системе	Может быть указан абсолютный или относительный путь в локальной системе. В том случае если путь явно не указан, экспортируемые файлы будут помещены в текущую директорию. Используется стандартный способ указания файла в UNIX
Сервер FTP	Используется следующий синтаксис для имя_файла: *ftp://пользователь@узел/файл_конфигурации*, где *пользователь* – это имя пользователя на узле, *узел* – это имя узла или IP-адрес сервера FTP, а *файл_конфигурации* – это файл конфигурации, включая путь. Если пользователь не указан, будет выдан запрос на его ввод. Если аутентификация производится по паролю, далее будет запрошен пароль.
Сервер SCP	Используется следующий синтаксис для имя_файла: scp://*пользователь@узел/файл_конфигурации* где *пользователь* – это имя пользователя на узле, узел – это имя узла или IP-адрес сервера SCP, а файл_конфигурации – это файл конфигурации, включая путь. Если *пользователь* не указан, будет выдан запрос на его ввод. Если аутентификация производится по паролю, далее будет запрошен пароль.
Сервер TFTP	Используется следующий синтаксис для параметра *имя_файла*: tftp://*узел/архив* где *узел* это имя узла или IP-адрес сервера TFTP, а *архив* это архив, содержащий сертификат субъекта, секретный ключ, сертификат УЦ, а также список отозванных сертификатов, включая путь относительно корневого каталога TFTP

ПРИМЕЧАНИЕ При использовании команды pki export certificate <имя> экспортируется секретный ключ, связанный с открытым ключом, указанным в сертификате. Секретный ключ должен храниться в тайне, и не должен передаваться третьим лицам.

12.4.33 pki export-pkcs12 certificate <имя_сертификата> password <пароль>

Экспорт сертификата субъекта, ключевой пары субъекта, сертификата УЦ, списка отозванных сертификатов в формате PKCS12.

Синтаксис

```
pki export-pkcs12 certificate <имя_сертификата> password <пароль>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_сертификата

Имя сертификата, который требуется экспортировать.

пароль

Пароль, который будет использоваться для защиты секретного ключа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет экспортировать сертификат субъекта, сертификат УЦ, секретный ключ субъекта, а также список отозванных сертификатов на флэш-накопитель в формате PKCS12.

Если в качестве объекта для экспорта указывается сертификат УЦ, а не сертификат субъекта, то список отозванных сертификатов и закрытый ключ УЦ не экспортируются, т.е. производится экспорт только сертификата УЦ.

PKCS#12 представляет собой стандарт семейства Public-Key Cryptography Standards (PKCS). Он определяет файловый формат, используемый для хранения секретных ключей в сопровождении с сертификатами, защищенный при помощи основанного на пароле симметричного ключа.

При выполнении данной команды к устройству должен быть подключен флэш-накопитель. Монтирование и размонтирование флэш-накопителя осуществляется автоматически. Экспортируемые файлы будут помещены в корневую директорию флэш-накопителя. К экспортируемым файлам относятся: сертификат формата PKCS#12 и список отзыва сертификатов (CRL) в отдельном файле.

ПРИМЕЧАНИЕ При использовании команды **pki export-pkcs12 certificate** <имя> экспортируется секретный ключ, связанный с открытым ключом, указанным в сертификате. Секретный ключ должен храниться в тайне, и не должен передаваться третьим лицам.

12.4.34 pki import

Импорт сертификата/сертификатов УЦ, сертификата субъекта, ключевой пары субъекта, сертификата УЦ, списка отозванных сертификатов.

Синтаксис

```
pki import [from <имя_файла>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_файла

Имя архива, содержащего сертификат субъекта, ключевую пару субъекта, сертификат УЦ и список отозванных сертификатов, если он необходим.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет импортировать сертификат субъекта, сертификат УЦ и секретный ключ субъекта, также при необходимости может быть импортирован список отозванных сертификатов. Поддерживается импорт сертификатов формата v3. При выполнении команды **pki import** без параметров к устройству должен быть подключен флэш-накопитель, в корневой директории которого должны размещаться следующие файлы:

- сертификат удостоверяющего центра;
- сертификат субъекта;
- секретный ключ субъекта.

При наличии в корневом разделе файла со списком отозванных сертификатов, для него осуществляется проверка подписи. В том случае если проверка подписи для данного списка отозванных сертификатов прошла успешно, а также этот список новее имеющегося в системе, он будет импортирован.

Если для сертификата субъекта отсутствует секретный ключ, сертификат будет импортирован, но выведется предупреждение об отсутствии данного ключа.

В том случае если в импортируемом сертификате УЦ присутствует расширение CRL Distribution Points, автоматически будет произведена попытка получить актуальный список отзыва сертификатов.

Монтирование и размонтирование флэш-накопителя осуществляется автоматически. В результате выполнения указанной команды в систему будут добавлены сертификат удостоверяющего центра, сертификат субъекта, подписанный указанным удостоверяющим центром, секретный ключ и список отозванных сертификатов (при его наличии).

Могут быть импортированы иерархические цепочки сертификатов. При импорте цепочки из более 2 сертификатов в конфигурационном файле будет отображен только корневой УЦ и конечные сертификаты субъектов.

При указании параметра **from** производится импорт сертификата из файла архива по указанному адресу, который может быть локальным или находиться на сервере TFTP, FTP или SCP. Поддерживаются архивы в формате tar.gz, tar.bz2 и zip.

В приведенной ниже таблице показан синтаксис указания файла для различных местоположений файла.

Таблица 60 – Способы указания местоположения для импорта сертификата

Местоположение	**Способ указания**
Путь в локальной системе	Может быть указан абсолютный или относительный путь в локальной системе. Используется стандартный способ указания файла в UNIX
Сервер FTP	Используется следующий синтаксис для параметра *имя_файла*: ftp://*пользователь*@*узел*/*архив*, где *пользователь* – это имя пользователя на узле, *узел* – это имя узла или IP-адрес сервера FTP, а *архив* - это название архива, содержащего сертификат субъекта, секретный ключ, сертификат УЦ, а также при необходимости файл, содержащий список отозванных сертификатов. Название должно включать путь к файлу. Если *пользователь* не указан, будет выдан запрос на его ввод. Если аутентификация производится по паролю, далее будет запрошен пароль.
Сервер SCP	Используется следующий синтаксис для *имя_файла*: scp://пользователь@узел/архив где *пользователь* - это имя пользователя на узле, *узел* это имя узла или IP-адрес сервера SCP, а *архив* - это архив, содержащий сертификат субъекта, секретный ключ, сертификат УЦ, а также при необходимости файл, содержащий список отозванных сертификатов. Название должно включать путь к файлу. Если *пользователь* не указан, будет выдан запрос на их ввод. Если аутентификация производится по паролю, далее будет запрошен пароль.
Сервер TFTP	Используется следующий синтаксис для параметра *имя_файла*: tftp://*узел*/*архив* где *узел* это имя узла или IP-адрес сервера TFTP, а *архив* - это архив, содержащий сертификат субъекта, секретный ключ, сертификат УЦ, а также при необходимости файл, содержащий список отозванных сертификатов. Название должно включать путь относительно корневого каталога TFTP

12.4.35 pki import-pkcs12 password <пароль>

Импорт сертификата субъекта, ключевой пары субъекта, сертификата УЦ в формате PKCS12 и списка отозванных сертификатов.

Синтаксис

```
pki import-pkcs12 password <пароль> [from <имя_файла>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

пароль

Пароль, который был указан при импорте сертификата в формате PKCS12.

имя_файла

Имя файла PKCS12, либо (при необходимости импорта списка отозванных сертификатов) имя архива, содержащего файл PKCS12 и файл со списком отозванных сертификатов. Поддерживаются архивы следующих форматов:zip, tar.bz2, tar.gz.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет импортировать с флэш-накопителя сертификат субъекта, сертификат УЦ, секретный ключ субъекта в формате PKCS12, а также список отозванных сертификатов. Поддерживается импорт сертификатов формата v3.

При выполнении команды **pki import-pkcs12 password <**пароль**>** к устройству должен быть подключен флэш-накопитель, в корне которого размещается файл в формате PKCS12 (имеющий расширение p12). Файл в формате PKCS12 содержит:

- сертификат удостоверяющего центра;
- сертификат субъекта;
- секретный ключ субъекта.

При наличии в корневом разделе файла со списком отозванных сертификатов, для него осуществляется проверка подписи. В том случае если проверка подписи для данного списка отозванных сертификатов прошла успешно, а также этот список новее имеющегося в системе, он будет импортирован.

Если для сертификата субъекта отсутствует секретный ключ, сертификат будет импортирован, но выведется предупреждение об отсутствии ключа.

В том случае если в импортируемом сертификате УЦ присутствует расширение CRL Distribution Points, автоматически будет произведена попытка получить актуальный список отзыва сертификатов.

Монтирование и размонтирование флэш-накопителя осуществляется автоматически. В результате выполнения указанной команды в систему будет добавлен сертификат удостоверяющего центра, сертификат субъекта, подписанный указанным удостоверяющим центром, секретный ключ, также может быть добавлен список отозванных сертификатов.

При указании параметра **from** производится импорт сертификата из файла по указанному адресу, который может быть локальным или находиться на сервере TFTP, FTP или SCP.

В приведенной ниже таблице показан синтаксис указания файла для различных местоположений файла.

ПРИМЕЧАНИЕ Сертификат в формате PKCS12 включает в себя секретный ключ субъекта, в связи с этим канал связи, по которому передается такой сертификат должен быть безопасным.

Таблица 61 – Способы указания местоположения для импорта сертификата

Местоположение	**Способ указания**
Путь в локальной системе	Может быть указан абсолютный или относительный путь в локальной системе. Используется стандартный способ указания файла в UNIX
Сервер FTP	Используется следующий синтаксис для параметра *имя_файла*: ftp://*пользователь*@*узел*/*имя_файла*, где *пользователь* – это имя пользователя на узле, *узел* – это имя узла или IP-адрес сервера FTP, а *имя_файла* - это: - название файла в формате PKCS12, содержащего сертификат субъекта, секретный ключ, сертификат УЦ. - название архива в формате zip/tar.bz2/tar.gz, содержащего файл PKCS12 и при необходимости файл со списком отозванных сертификатов. Если *пользователь* и *пароль* не указаны, будет выдан запрос на их ввод
Сервер SCP	Используется следующий синтаксис для *имя_файла*: scp://пользователь@узел/имя_файла где *пользователь* это имя пользователя на узле, *узел* это имя узла или IP-адрес сервера

Местоположение	Способ указания
	SCP, а *имя_файла* - это: - название файла в формате PKCS12, содержащего сертификат субъекта, секретный ключ, сертификат УЦ; - название архива в формате zip/tar.bz2/tar.gz, содержащего файл PKCS12 и при необходимости файл со списком отозванных сертификатов. Если *пользователь* не указан, будет выдан запрос на его ввод. Если аутентификация производится по паролю, далее будет запрошен пароль.
Сервер TFTP	Используется следующий синтаксис для параметра *имя_файла*: tftp://*узел*/*имя_файла* где *узел* это имя узла или IP-адрес сервера TFTP, а *имя_файла* - - это: - название файла в формате PKCS12, содержащего сертификат субъекта, секретный ключ, сертификат УЦ; - название архива в формате zip/tar.bz2/tar.gz, содержащего файл PKCS12 и при необходимости файл со списком отозванных сертификатов. Название указывается включая путь относительно корневого каталога TFTP

12.4.36 pki revoke ca <имя> certificate <имя_сертификата>

Команда для отзыва сертификата.

Синтаксис

```
pki revoke ca <имя> certificate <имя_сертификата>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя

Имя удостоверяющего центра, который выпустил отзываемый сертификат.

имя_сертификата

Имя отзываемого сертификата.

Значение по умолчанию

Отсутствует.

Указания по использованию

Сертификат может быть отозван только в том случае, если на устройстве присутствует закрытый ключ удостоверяющего центра, подписавшего данный сертификат.

При выполнении команды, указанный сертификат помечается как отозванный:

- в конфигурационном режиме для указанного сертификата добаляется параметр *status* со значением *revoked;*
- для удостоверяющего центра обновляется список отзыва сертификатов (CRL).

ПРИМЕЧАНИЕ: В конфигурационном режиме запрещено изменять параметр *status* для сертификатов. При попытке изменения параметра будет возвращено сообщение об ошибке:

```
[edit]
admin@edge#set pki ca RootCA certificate TestCert1 status revoked
[edit]
admin@edge# commit
E: Служебное поле status не может быть установлено пользователем
Commit failed
[edit]
admin@edge#
```

12.4.37 pki update-crl

Обновление списка отозванных сертификатов для УЦ, в сертификате которых присутствует расширение CRLDistributionPoints.

Синтаксис

```
pki update-crl [<имя_УЦ>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_УЦ

Имя удостоверяющего центра, для которого требуется обновить CRL.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет обновить список отзыва сертификатов для УЦ, в котором присутствует расширение CRLDistributionPoints.

В том случае если в импортируемом сертификате УЦ присутствует расширение CRLDistributionPoints, автоматически будет произведена попытка получить актуальный список отзыва сертификатов. Впоследствии обновить список отзыва сертификатов можно при помощи данной команды.

В том случае если имя УЦ, для которого требуется обновить список отозванных сертификатов, явно не указано, обновление будет осуществляться для всех сертификатов УЦ, известных модулю PKI, в которых присутствует расширение CRLDistributionPoints.

13 SSH

13.1 Настройка SSH

Протокол SSH (Secure Shell) обеспечивает безопасный механизм входа в систему Edge и получения доступа к интерфейсу командной строки. В поставляемом Numa edge по умолчанию настроен сервис SSH на управляющем интерфейсе на стандартном для SSH порту (22). По умолчанию управляющий порт Edge настроен на сеть 192.168.200.0/24 и имеет собственный адрес 192.168.200.1. При подключении к управляющему порту настройки автоматически выдаются сервером DHCP.

При необходимости, можно также настроить этот сервис для других интерфейсов, что обеспечит безопасный удаленный доступ к системе. В дополнение к стандартной аутентификации по паролю, используемой службой SSH, также может использоваться аутентификация по совместно используемым открытым ключам. Настройка SSH доступна администратору безопасности комплекса. Пользователь может использовать форму **show** описанных ниже команд для отображения настроек.

13.2 Команды SSH

Команды настройки	
service ssh active <состояние>	Возможность отключения сервиса SSH с сохранением настройки.
service ssh address <адрес> port <порт>	Включение SSH как протокола доступа в систему МЭ на определённом адресе и порту.
service ssh cipher <алгоритм>	Указание допустимых для использования алгоритмов шифрования.
service ssh client-alive-timeout <время>	Указание времени ожидания активности клиента.
service ssh disable-password-authentication	Отключение парольной аутентификации при получении доступа по протоколу SSH.
service ssh hmac <алгоритм>	Указание допустимых для использования алгоритмов выработки имитовставки.
service ssh key-exchange-algo <алгоритм>	Указание допустимых для использования алгоритмов обмена ключами.

Эксплуатационные команды отсутствуют.

13.2.1 service ssh active <состояние>

Возможность отключения сервиса SSH с сохранением настройки.

Синтаксис

```
set service ssh active <состояние>
delete service ssh active
show service ssh active
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   ssh {
      active состояние
   }
}
```

Параметры

состояние

Административное состояние сервиса SSH. Поддерживаются следующие значения:

on: Включение сервиса SSH.

off: Отключение сервиса SSH без отбрасывания настройки.

Значение по умолчанию

Сервис SSH включен.

Указания по использованию

Эта команда используется для отключения сервиса SSH с сохранением настройки.

Форма **set** данной команды используется для указания состояния сервиса SSH.

Форма **delete** данной команды используется для восстановления значения по умолчанию.

Форма **show** данной команды используется для отображения состояния сервиса SSH.

13.2.2 service ssh address <адрес> port <порт>

Включение SSH как протокола доступа в систему МЭ на определённом адресе и порту.

Синтаксис

```
set service ssh address <адрес> [port <порт>]
delete service ssh address <адрес> [port]
show service ssh address <адрес> [port]
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   ssh {
      address адрес {
         port порт
      }
   }
}
```

Параметры

адрес

Множественный узел. IPv4-адрес, на котором будет принимать соединения сервис SSH.

порт

Номер порта, который будет использоваться службой SSH. Значение должно лежать в диапазоне **1-65535**.

Значение по умолчанию

По умолчанию используется порт номер 22.

Указания по использованию

Команда используется для разрешения приема запросов SSH от удаленных систем на конкретных адресах локальной системы. Позволяется указание нескольких адресов. Также в качестве адреса может быть указано значение 0.0.0.0, подразумевающее ожидание входящих SSH соединений на любом адресе. При использовании значения 0.0.0.0 не поддерживаются иные значения узла **service ssh address <адрес>**.

Создание узла конфигурации адреса SSH делает возможным использование протокола SSH для получения доступа к системе по указанному адресу. По умолчанию маршрутизатор использует для службы SSH порт 22. Поддерживается только вторая версия протокола SSH.

Форма **set** данной команды используется для указания адреса, на котором будет принимать соединения сервис SSH.

Форма **delete** данной команды используется для удаления адреса, на котором будет принимать соединения сервис SSH.

Форма **show** данной команды используется для отображения настройки прослушиваемых адресов сервиса SSH.

13.2.3 service ssh cipher <алгоритм>

Указание допустимых для использования алгоритмов шифрования.

Синтаксис

```
set service ssh cipher <алгоритм>

delete service ssh cipher <алгоритм>

show service ssh cipher
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   ssh {
      cipher алгоритм
   }
}
```

Параметры

алгоритм

Формат – текст. Допустимый для использования протоколом SSH алгоритм шифрования. Множественный узел.

Список поддерживаемых алгоритмов:

- **aes128-cbc, aes128-ctr** - AES (Advanced Encryption Standard) с ключом 128 бит.
- **aes192-cbc, aes192-ctr** - AES (Advanced Encryption Standard) с ключом 192 бит.
- **aes256-cbc, aes256-ctr** - AES (Advanced Encryption Standard) с ключом 256 бит.
- **arcfour** - Alleged RC4 с ключом 128 бит.
- **arcfour128, arcfour256** - Alleged RC4 с ключом 128 / 256 бит (с дополнениями RFC 4345).
- **blowfish-cbc** - Blowfish с ключом 128 бит.
- **cast128-cbc** - CAST-128 с ключом 128 бит.
- **gost89-cbc, gost89-ctr, gost89-cfb, gost89-ofb** - шифрование на основе алгоритма, определенного ГОСТ 28147-89.
- **kuznechik-cbc, kuznechik-ctr, kuznechik-cfb, kuznechik-ofb** - шифрование на основе алгоритма "Кузнечик" (ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015).

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания допустимых для использования алгоритмов симметричного шифрования. Для работы сервиса SSH должен быть настроен хотя бы один алгоритм шифрования. Изначально в изделии настроен алгоритм kuznechik-ofb.

Форма **set** данной команды используется для задания алгоритмов шифрования.

Форма **delete** данной команды используется для удаления заданных алгоритмов.

Форма **show** данной команды используется для просмотра настройки.

13.2.4 service ssh client-alive-timeout <время>

Указание времени ожидания активности клиента.

Синтаксис

```
set service ssh client-alive-timeout <время>
delete service ssh client-alive-timeout
show service ssh client-alive-timeout
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    ssh {
        client-alive-timout время
    }
}
```

Параметры

время

Время (в секундах), по истечению которого происходит отключение неактивного соединения с клиентом SSH. Значение лежит в диапазоне от 0 до 2147483647.

Значение по умолчанию

По умолчанию отключение неактивного соединения с клиентом SSH происходит по истечению 1800 секунд.

Указания по использованию

Эта команда используется для указания времени, по истечению которого происходит отключение неактивного соединения с клиентом SSH (таймаут соединения). При указании значения 0 отключение неактивного соединения с клиентом SSH не происходит.

Форма **set** данной команды используется для задания рассматриваемого параметра.

Форма **delete** данной команды используется для удаления параметра и использования значения по умолчанию.

Форма **show** данной команды используется для просмотра настройки.

13.2.5 service ssh disable-password-authentication

Отключение парольной аутентификации при получении доступа по протоколу SSH.

Синтаксис

```
set service ssh disable-password-authentication
delete service ssh disable-password-authentication
show service ssh
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    ssh {
        disable-password-authentication
    }
}
```

Параметры

Отсутствуют

Значение по умолчанию

Парольная аутентификация включена.

Указания по использованию

ПРЕДУПРЕЖДЕНИЕ Прежде чем отключать парольную аутентификацию, рекомендуется настроить аутентификацию с использованием общих открытых ключей, иначе возможна потеря доступа к системе по протоколу SSH.

Команда запрещает парольную аутентификацию для пользователей SSH. Как правило, используется при настроенной аутентификации с использованием общих открытых ключей. Аутентификация с использованием общих открытых ключей значительно менее чувствительна к подбору ключа, в отличие от подбора пароля.

Форма **set** данной команды используется для задания рассматриваемого параметра.

Форма **delete** данной команды используется для удаления параметра и использования значения по умолчанию.

Форма **show** данной команды используется для просмотра настройки.

13.2.6 service ssh hmac <алгоритм>

Указание допустимых для использования алгоритмов выработки имитовставки.

Синтаксис

```
set service ssh hmac <алгоритм>

delete service ssh hmac <алгоритм>

show service ssh hmac
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    ssh {
        hmac алгоритм
    }
}
```

Параметры

алгоритм

Формат – текст. Допустимый для использования протоколом SSH алгоритм выработки имитовставки. Множественный узел.

Список поддерживаемых алгоритмов (хеш-функций):

- **hmac-md5** - алгоритм MD5 (Message Digest) с хешем 128 бит.
- **hmac-md5-96** - алгоритм на основе MD5 с хешем 96 бит.
- **hmac-sha1** - алгоритм SHA1 (Secure Hash Algorithm) с хешем 128 бит.
- **hmac-sha1-96** - алгоритм на основе SHA1 с хешем 96 бит.
- **hmac-ripemd160** - алгоритм RIPEMD (RACE Integrity Primitives Evaluation Message Digest) с хешем 160 бит.
- **hmac-ripemd160@openssh.com** - алгоритм RIPEMD с хешем 160 бит в реализации проекта OpenSSH.
- **umac-64@openssh.com** - алогритм UMAC (universal hashing).
- **hmac-gosthash** - алгоритм на основе ГОСТ Р 34.11-94 .
- **hmac-stribog-256, hmac-stribog-512** - алгоритм на основе ГОСТ Р 34.11-2012 с хешем 256 / 512 бит соответственно.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания допустимых для использования алгоритмов выработки имитовставки. Для работы сервиса SSH должен быть настроен хотя бы один алгоритм выработки имитовставки. Изначально в изделии настроены алгоритмы hmac-stribog-256 и hmac-stribog-512.

Форма **set** данной команды используется для задания алгоритмов выработки имитовставки.

Форма **delete** данной команды используется для удаления заданных алгоритмов.

Форма **show** данной команды используется для просмотра настройки.

13.2.7 service ssh key-exchange-algo <алгоритм>

Указание допустимых для использования алгоритмов обмена ключами.

Синтаксис

```
set service ssh key-exchange-algo <алгоритм>
delete service ssh key-exchange-algo <алгоритм>
show service ssh key-exchange-algo
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   ssh {
      key-exchange-algo алгоритм
   }
}
```

Параметры

алгоритм

Формат – текст. Допустимый для использования сервером SSH алгоритм обмена ключами. Множественный узел.

Список поддерживаемых алгоритмов:

- diffie-hellman-group-exchange-sha1;
- diffie-hellman-group-exchange-sha256;
- diffie-hellman-group1-sha1;
- diffie-hellman-group14-sha1;
- ecdh-gost2012-256-cpa;
- ecdh-gost2012-256-cpb.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания допустимых для использования алгоритмов ключевого обмена. Для работы сервиса SSH должен быть настроен хотя бы один алгоритм ключевого обмена. Изначально в изделии настроен алгоритм ecdh-gost2012-256-cpa.

Форма **set** данной команды используется для задания алгоритмов ключевого обмена.

Форма **delete** данной команды используется для удаления заданных алгоритмов.

Форма **show** данной команды используется для просмотра настройки.

14 Настройка доступа к Web-интерфейсу

14.1 Настройка HTTP_HTTPS

Безопасный механизм входа в систему Numa Edge и получения доступа к графическому пользовательскому Web-интерфейсу обеспечивается при помощи HTTPS (HTTP Secure), который представляет собой расширение протокола HTTP, использующее подключения на основе SSL/TLS.

По умолчанию доступ к Web-интерфейсу разрешен на управляющем интерфейсе (192.168.200.1) на портах 80 (HTTP) и 443 (HTTPS). Для обеспечения безопасного соединения доступ к Web-интерфейсу осуществляется при помощи HTTPS. Для совместимости Web-сервер принимает также HTTP трафик на порту 80, который автоматически перенаправляется на порт 443 (HTTPS). Для того чтобы обеспечить возможность подключений на базе HTTPS, в системе Numa Edge должен быть в указан используемый Web-сервером сертификат.

По умолчанию в системе Numa Edge предустановлен удостоверяющий центр, на базе которого создан и заверен сертификат Web-сервера. Вследствие этого при получении доступа к Web-интерфейсу может быть выдано предупреждение системы безопасности о том, что сертификат узла подписан неизвестным удостоверяющим центром. В этом случае следует подтвердить согласие на открытие узла, после чего страница продолжит загружаться.

При необходимости можно также настроить доступ к Web-интерфейсу на других интерфейсах системы, изменить номера сетевых портов на которых принимаются подключения, а также изменить сертификат Web-сервера.

По умолчанию для аутентификации Web-сервера используется криптографический алгоритм на основе стандарта ГОСТ 34.10-2012, для шифрования передаваемых данных используется криптографические алгоритмы на основе стандартов ГОСТ 34.12-2018, ГОСТ 34.13-2018. По этой причине необходимо использовать браузер, который поддерживает данный набор криптографических алгоритмов.

14.1.1 Настройка доступа к Web-интерфейсу с использованием стороннего сертификата

В приведенном примере разрешается доступ к Web-интерфейсу по заранее настроенному в системе адресу 192.168.10.1, а также выполняется замена сертификата, используемого по умолчанию, на сертификат, созданный сторонним удостоверяющим центром.

Пример 126– Разрешение доступа к Web-интерфейсу по указанному адресу с использованием стороннего сертификата

Действие	**Команда**
В операционном режиме выполняется импорт сертификата веб-сервера, сгенерированного сторонним УЦ, с подключенного флэш-накопителя.	admin@edge:~$ pki import from WebCert.tgz Импортируется сертификат УЦ Web CA как webca Импортируется сертификат Web Cert как webcert Импортируется CRL для webca Импортируется ключ для webcert admin@edge:~$

Отображение импортированного сертификата в режиме конфигурирования.	[edit]
	admin@edge# show pki ca webca
	certificate webcert {
	cn "Web Cert"
	expires-on "Sat Dec 17 12:58:22 2022"
	}
	cn "Web CA"
	expires-on "Sat Jun 17 12:58:20 2023"
	key-size 4096
	key-type rsa
	last-update "Fri Jun 17 12:58:20 2022"
	next-update "Sat Jun 17 12:58:20 2023"

Указание адреса, который будет прослушиваться на предмет входящих подключений.	[edit] admin@edge# set service https address 192.168.10.1

Действие	Команда
Указание имени сертификата, который будет использоваться для подключения к Web-интерфейсу с использованием HTTPS.	`[edit]` `admin@edge# set service https x509-cert webcert`
Фиксация настройки.	`[edit]` `admin@edge# commit`

Просмотр настроек сервиса HTTPS.	`[edit]`
	`admin@edge# show service https`
	`address 192.168.10.1 {`
	`https-port 443`
	`www-port 80`
	`}`
	`x509-cert webcert`

14.2 Команды HTTP_HTTPS

Команды настройки	
service https address <адрес>	Включение доступа к Web-интерфейсу на определённом адресе.
service https address <адрес> https-port <порт>	Указание номера сетевого порта, который будет прослушиваться на предмет входящих запросов HTTPS .
service https address <адрес> www-port <порт>	Указание номера сетевого порта, который будет прослушиваться на предмет входящих запросов HTTP .
service https x509-cert <имя_сертификата>	Указание сертификата Web-сервера, используемого для проверки подлинности при получении доступа к Web-интерфейсу.

14.2.1 service https address <адрес>

Включение доступа к Web-интерфейсу Numa Edge на определённом адресе.

Синтаксис

```
set service https address <адрес>
delete service https address <адрес>
show service https address <адрес>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   https {
      address адрес {
      }
   }
}
```

Параметры

адрес

ipv4-адрес. Адрес, на котором будут приниматься запросы HTTP/HTTPS.

Значение по умолчанию

По умолчанию доступ к Web-интерфейсу возможен на управляющем интерфейсе (адрес 192.168.200.1).

Указания по использованию

Команда используется для разрешения приема запросов HTTP/HTTPS от удаленных систем на конкретных адресах локальной системы.

Создание узла конфигурации адреса веб-интерфейса делает возможным использование протоколов HTTP/HTTPS для получения доступа к системе по этому адресу. По умолчанию используется безопасный механизм доступа к веб-интерфейсу на основе протокола HTTPS.

ПРИМЕЧАНИЕ Адрес должен быть заранее определен в системе.

Форма **set** данной команды используется для создания настройки адреса веб-интерфейса.

Форма **delete** данной команды используется для удаления настройки адреса веб-интерфейса.

ПРИМЕЧАНИЕ При удалении узла конфигурации адреса веб-интерфейса доступ к системе по HTTP/HTTPS будет отключен на всех портах, за исключением управляющего.

Форма **show** данной команды используется для отображения настройки прослушиваемых адресов веб-сервера.

14.2.2 service https address <адрес> https-port <порт>

Включение доступа к Web-интерфейсу Numa Edge по протоколу HTTPS на определённом адресе и сетевом порту.

Синтаксис

```
set service https address <адрес> https-port <порт>
delete service https address <адрес> https-port
show service https address <адрес> https-port
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    https {
        address адрес {
            https-port порт
        }
    }
}
```

Параметры

адрес

ipv4-адрес. Адрес, на котором будут приниматься запросы HTTPS.

порт

Номер сетевого порта, на котором будут приниматься запросы HTTPS. Принимает значения в диапазоне 1-65535.

Значение по умолчанию

По умолчанию доступ к Web-интерфейсу возможен на управляющем интерфейсе (адрес 192.168.200.1) и сетевом порту 443.

Указания по использованию

Команда используется для разрешения приема запросов HTTPS от удаленных систем на указанных сетевых портах на конкретных адресах локальной системы. Для того чтобы веб-сервер принимал подключения HTTPS на указанном порту, в системе должен быть настроен доступ к веб-серверу на основе HTTPS (используемый сертификат веб-сервера указан при помощи команды service https x509-cert <имя_сертификата>).

Форма **set** данной команды используется для указания сетевого порта, на котором будут приниматься запросы HTTPS.

Форма **delete** данной команды используется для удаления текущей настройки и восстановления значения, принятого по умолчанию/

Форма **show** данной команды используется для отображения настройки.

14.2.3 service https address <адрес> www-port <порт>

Указание сетевого порта, на котором будут приниматься запросы HTTP.

Синтаксис

```
set service https address <адрес> www-port <порт>
delete service https address <адрес> www-port
show service https address <адрес> www-port
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   https {
      address адрес {
         www-port порт
      }
   }
}
```

Параметры

адрес

ipv4-адрес. Адрес, на котором будут приниматься запросы HTTP.

порт

Номер сетевого порта, на котором будут приниматься запросы HTTP. Принимает значения в диапазоне 1-65535.

Значение по умолчанию

По умолчанию используется сетевой порт 80.

Указания по использованию

Команда используется для разрешения приема запросов HTTP от удаленных систем на указанных сетевых портах на конкретных адресах локальной системы.

Для обеспечения безопасности передаваемых данных по умолчанию доступ к Web-интерфейсу возможен только с использованием HTTPS. При получении запроса HTTP на указанном сетевом порту произойдет автоматическое перенаправление на порт, указанный при помощи команды **service https address <адрес> https-port** (по умолчанию 443), после чего дальнейшее взаимодействие будем осуществляться с использованием HTTPS. Если в системе настроен доступ к веб-серверу на основе HTTP, то есть используемый сертификат веб-сервера не указан, доступ к веб-интерфейсу осуществляется по протоколу HTTP на указанном порту.

Форма **set** данной команды используется для указания сетевого порта на котором будут приниматься запросы HTTP.

Форма **delete** данной команды используется для удаления настройки HTTP.

Форма **show** данной команды используется для отображения настройки.

14.2.4 service https x509-cert <имя_сертификата>

Указание имени сертификата Web-сервера, используемого для проверки подлинности при подключении к Web-интерфейсу Numa Edge.

Синтаксис

```
set service https x509-cert <имя_сертификата>
delete service https x509-cert
show service https x509-cert
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   https {
      x509-cert имя_сертификата
   }
}
```

Параметры

имя_сертификата

Обязательный. Имя сертификата Web-сервера, используемого для проверки подлинности.

Значение по умолчанию

По умолчанию в системе Numa Edge предустановлен удостоверяющий центр (CN = Default Edge CA), на базе которого создан и заверен сертификат Web-сервера (CN=Numa edge Web Interface), использующий открытый ключ криптографического алгоритма ГОСТ 34.10-2001.

Указания по использованию

Данная команда позволяет указать сертификат, который будет использоваться для подключения с использованием HTTPS к Web-интерфейсу Numa Edge. Если используемый сертификат не указан, доступ к веб-интерфейсу осуществляется по протоколу HTTP.

Может быть использован как сертификат созданный при помощи модуля PKI, так и сертификат, созданный при помощи стороннего удостоверяющего центра. В этом случае сертификат необходимо предварительно импортировать в систему при помощи команды **pki import**. Тип открытого ключа, указанного в сертификате, определяет набор криптографических алгоритмов, которые используются для обеспечения безопасности передаваемых данных.

Удаление конфигурации используемого сертификата не рекомендуется, так как в этом случае взаимодействие с веб-сервером будет устанавливаться через небезопасное соединение по протоколу HTTP.

Форма **set** данной команды используется для указания имени сертификата, используемого для подключения к Web-интерфейсу Numa Edge при помощи HTTPS.

Форма **delete** данной команды используется для удаления настройки используемого имени сертификата, в этом случае для взаимодействия с сервером используется протокол HTTP.

Форма **show** данной команды используется для отображения настройки используемого имени сертификата.

15 Учет сетевого трафика

15.1 Настройка системы учета сетевого трафика

15.1.1 Экспорт данных учета сетевого трафика

В дополнение к локальному выводу, существует возможность экспортировать данные учета сетевого трафика на сервер сбора данных NetFlow или sFlow. В следующем примере приведена настройка экспорта данных учета сетевого трафика в формате NetFlow на удаленный сервер сбора данных с IP-адресом 192.168.10.150 и портом по умолчанию.

Пример 127– Экспорт данных в формате NetFlow на узел 192.168.10.150

Действие	**Команда**
Настройка экспорта данных в формате NetFlow на узел 192.168.10.150	`[edit]` `admin@edge# set service flow-accounting netflow server 192.168.10.150`
Фиксация настройки	`[edit]` `admin@edge# commit`

Отображение настройки	`[edit]`
	`admin@edge# show service flow-accounting`
	`  interface eth1`
	`  netflow {`
	`  server 192.168.10.150 {`
	`  }`
	`  }`

15.1.2 Вывод данных учета сетевого трафика

После того, как на выбранном интерфейсе был включен учет сетевого трафика, появляется возможность вывода сведений о сетевом трафике на основе:

- интерфейса;
- сетевого узла;
- сетевого порта;
- объема сетевого трафика.

В примере ниже приведен вывод данных учета сетевого трафика для интерфейса **eth1**.

Информация о принадлежности IP-адресов, приведенных в выводе:

- 192.168.10.1 - Numa Edge;
- 192.168.10.2, 192.168.10.3, 192.168.10.4 - клиентские компьютеры;
- 192.168.10.254 - основной шлюз;
- 192.168.10.255 - широковещательный адрес;
- 192.168.20.11, 192.168.20.22 - DNS-серверы;
- 8.8.8.8 - Google Public DNS.

Пример 128– Вывод данных учета сетевого трафика для интерфейса eth1

```
admin@edge:~$ service flow-accounting show interface eth1
running
flow-accounting for [eth1]
Src Addr         Dst Addr         Sport Dport Proto    Packets      Bytes
Flows
192.168.10.2     192.168.10.1     5057  22      tcp          34       6172
1
192.168.10.2     192.168.10.255   137   137     udp          69       5382
6
192.168.10.2     192.168.10.255   63982 1947    udp          75       5100
1
```

```
192.168.10.3    192.168.10.255  138   138     udp          12        2904
6
192.168.10.2    192.168.10.1    5058  22      tcp          17        1560
1
8.8.8.8         192.168.10.1    0     0       icmp         13        1092
1
192.168.10.2    192.168.10.1    0     0       icmp         11         924
1
192.168.10.254  192.168.10.1    0     0       icmp          7         588
1
192.168.10.4    192.168.10.1    0     0       icmp          6         504
2
192.168.20.22   192.168.10.1    53    22365   udp           1         146
1
192.168.20.11   192.168.10.1    53    22365   udp           1         138
1
192.168.20.22   192.168.10.1    53    8845    udp           1         131
1
192.168.20.11   192.168.10.1    53    8845    udp           1         123
1

Total entries: 13
Total flows  : 24
Total pkts   : 248
Total bytes  : 24,764
```

В следующем примере приведен вывод данных учета сетевого трафика для узла 192.168.10.2 на интерфейсе **eth1**.

Пример 129– Вывод данных учета сетевого трафика для узла 192.168.10.2 на интерфейсе eth1

```
admin@edge:~$ service flow-accounting show interface eth1 host 192.168.10.2
running
Src Addr         Dst Addr         Sport Dport Proto    Packets      Bytes
Flows
192.168.10.2    192.168.10.1    5057  22      tcp          34        6172
1
192.168.10.2    192.168.10.255  137   137     udp          69        5382
6
192.168.10.2    192.168.10.255  63982 1947    udp          75        5100
1
192.168.10.2    192.168.10.1    5058  22      tcp          17        1560
1
192.168.10.2    192.168.10.1    0     0       icmp         11         924
1

Total entries: 5
Total flows  : 10
Total pkts   : 206
Total bytes  : 19,138
```

15.1.3 Настройка интерфейса для учета сетевого трафика

В данном разделе приведена настройка учета сетевых потоков на интерфейсе eth1.

Для включения учета сетевых потоков на интерфейсе нужно выполнить следующие действия в режиме настройки.

Пример 130- Настройка интерфейса для учета сетевого трафика

Действие	**Команда**
Настройка учета сетевого трафика на интерфейсе eth1	`[edit]` `admin@edge# set service flow-accounting`

	`interface eth1`
Фиксация настройки	`[edit]` `admin@edge# commit`

Отображение настройки	`[edit]`
	`admin@edge# show service`
	`flow-accounting {`
	`interface eth1`
	`}`

15.1.4 Общие сведения о системе учета сетевого трафика

Numa Edge предоставляет механизм по сбору статистики и предоставлению отчетов о сетевом трафике. Данные учета могут быть выведены как локально, так и экспортированы на удаленные сервера сбора и анализа данных. Numa Edge поддерживает учет данных в формате NetFlow или sFlow.

Протокол NetFlow

NetFlow — сетевой протокол, предназначенный для учёта сетевого трафика, разработанный компанией Cisco Systems. NetFlow предоставляет администраторам доступ к информации о потоках IP в сети передачи данных. Поток данных определяется как однонаправленная последовательность пакетов с неким общим набором свойств, проходящих через сетевое устройство.

Для сбора информации о трафике по протоколу NetFlow требуются следующие компоненты:

- *экспортер* - собирает статистику по проходящему через него трафику, объединяет пакеты в потоки и экспортирует записи потоков в один или несколько коллекторов (сборщиков) потоков;
- *коллектор* - собирает получаемые от экспортера данные и помещает их в хранилище;
- *анализатор* - анализирует собранные коллектором данные и формирует пригодные для чтения человеком отчёты.

Экспортер выделяет из проходящего трафика *потоки*, характеризуемые следующими параметрами:

- входящий интерфейс;
- IP-адрес источника;
- IP-адрес получателя;
- порт источника для протоколов UDP или TCP, 0 для остальных протоколов;
- порт получателя для протоколов UDP иили TCP, тип и код для ICMP, 0 для остальных протоколов;
- протокол IP;
- тип обслуживания IP-пакетов.

Каждый отдельный сеанс TCP с идентичными параметрами сетевого потока учитывается в статистике как новый сетевой поток. Поток TCP считается завершенным, если заканчивается сеанс или истекает время ожидания для потока. Может быть настроено несколько интервалов ожидания (таймаут), по истечении которых сетевой поток считается завершенным.

Для сетевых протоколов без установления соединения таких как ICMP и UDP, сетевой поток считается завершенным если в течение указанного интервала ожидания не принят ни один пакет, относящийся к данному потоку.

Включение учета сетевого трафика осуществляется отдельно для каждого интерфейса. Все пакеты, полученные на интерфейсе, будут учтены и представлены в статистических данных для интерфейса. При этом следует учитывать, что просмотр всех пакетов потребует значительных вычислительных ресурсов. В качестве альтернативы, позволяющей снизить нагрузку на систему, можно учитывать каждый n-ный пакет (n – частота выборки), и производить оценку на основе выбранных пакетов. Это позволит снизить потребляемые ресурсы по сравнению с учетом всех пакетов, при этом обеспечивая приемлемую точность.

Протокол sFlow

sFlow — технология мониторинга трафика в сетях.

Система мониторинга sFlow включает следующие компоненты:

- *агент* — обеспечивает интерфейс для настройки измерительного процесса, связанного с источником

данных на устройстве, отвечает за поддержку сеансов измерения с коллекторами sFlow, собирает учетные данные в дейтаграммы sFlow для передачи коллекторам;
- *коллектор* — получает дейтаграммы sFlow от одного или множества агентов sFlow.

Архитектура и методы выборки, используемые в системе мониторинга sFlow, были разработаны для обеспечения непрерывного мониторинга трафика в масштабе сайта (и предприятия) высокоскоростных сетей. В частности, было уделено особое внимание:

- точности мониторинга при гигабитных и более высоких скоростях;
- расширяемости системы до десятков тысяч агентов на один коллектор sFlow;
- обеспечения максимально низкой стоимости реализации агентов sFlow.

Агент sFlow использует технологию выборки для сбора статистики трафика с обслуживаемого агентом устройства. Выборка из потока пакетов означает произвольный (случайный) отбор части потока, наблюдаемой в источнике данных. Использование выборки необходимо для достижения масштабируемости. Основываясь на определенной частоте выборки n, в среднем 1 из n пакетов, наблюдаемых в источнике данных, попадет в выборку. Этот тип выборки не дает 100% точного результата, но он дает результат с количественной точностью. По этой причине sFlow применим к высокоскоростным сетям (скорость передачи гигабит в секунду и выше).

15.2 Команды системы учета сетевого трафика

Команды настройки	
service flow-accounting interception-point <точка_перехвата_трафика>	Указание точки, с которой будет вестись учет входящего сетевого трафика.
service flow-accounting interface <интерфейс>	Указание интерфейса, для которого будет производиться учет входящего трафика.
service flow-accounting netflow engine-id <идентификатор>	Указание идентификатора системы ID, которое будет включено в данные NetFlow.
service flow-accounting netflow max-flows <количество_потоков>	Указание максимального количества потоков.
service flow-accounting netflow sampling-rate <частота_выборки>	Указание частоты регистрации событий для NetFlow, с которой сетевые пакеты будут учитываться в статистике.
service flow-accounting netflow server <адрес>	Указание сервера сбора данных об учете трафика для экспорта данных NetFlow.
service flow-accounting netflow timeout expiry-interval <интервал>	Указание интервала, через который будут отправляться отчеты сборщику данных NetFlow.
service flow-accounting netflow timeout flow-generic <таймаут>	Указание таймаута сетевого потока для трафика IP.
service flow-accounting netflow timeout icmp <таймаут>	Указание таймаута сетевого потока для трафика ICMP.
service flow-accounting netflow timeout max-active-life <время_жизни>	Указание максимального интервала времени, в течении которого будет учитываться трафик, относящийся к сетевому потоку.
service flow-accounting netflow timeout tcp-fin <таймаут>	Указание таймаута сетевого потока TCP после получения пакета TCP с флагом FIN.
service flow-accounting netflow timeout tcp-generic <таймаут>	Указание таймаута сетевого потока TCP.
service flow-accounting netflow timeout tcp-rst <таймаут>	Указание таймаута сетевого потока TCP после получения пакета TCP с флагом RST.
service flow-accounting netflow timeout udp <таймаут>	Указание таймаута сетевого потока для трафика UDP.
service flow-accounting netflow version <версия>	Указание формата NetFlow, в котором будут экспортированы данные учета.
service flow-accounting sflow agent-address <адрес>	Указание IP-адреса агента sFlow.
service flow-accounting sflow sampling-rate	Указание частоты выборки для статистики sFlow.

<частота_выборки>	
service flow-accounting sflow server <адрес>	Указание адреса сборщика sFlow для экспорта данных учета.
service flow-accounting syslog-facility <источник>	Указание типов сообщений, относящихся к учету трафика, которые будут регистрироваться в журнале.
Эксплуатационные команды	
service flow-accounting clear counters	Очистка всех счетчиков учета трафика.
service flow-accounting show	Отображение статистики для всех интерфейсов, на которых ведется учет трафика.
service flow-accounting restart	Перезапуск службы учета сетевого трафика.

15.2.1 service flow-accounting interception-point <точка_перехвата_трафика>

Указание точки, с которой будет вестись учет входящего сетевого трафика: до межсетевого экрана, либо после.

Синтаксис

```
set service flow-accounting interception-point <точка_перехвата_трафика>
delete service flow-accounting interception-point
show service flow-accounting interception-point
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   flow-accounting {
      interception-point точка_перехвата_трафика
   }
}
```

Параметры

точка_перехвата_трафика

Точка перехвата сетевого трафика. Переключатель, указывающий точку перехвата входящего сетевого трафика. Допустимые значения:

post-fw: Учет начинает вестись после межсетевого экрана;

pre-fw: Учет начинает вестись перед межсетевым экраном.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет настроить точку, с которой будет вестись запись статистических данных о сетевых потоках.

Форма **set** данной команды используется для указания точки учета входящего трафика.

Форма **delete** данной команды используется для отключения точки учета входящего трафика.

Форма **show** данной команды используется для отображения точки учета входящего трафика.

15.2.2 service flow-accounting interface <интерфейс>

Указание интерфейса, для которого будет производиться учет входящего трафика.

Синтаксис

```
set service flow-accounting interface <интерфейс>
delete service flow-accounting interface <интерфейс>
```

```
show service flow-accounting interface
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    flow-accounting {
        interface интерфейс
    }
}
```

Параметры

интерфейс

Множественный узел. Интерфейс, для которого будет осуществляться учет входящего трафика (например, eth0). Интерфейс доджен быть заранее настроен в системе.

Для того чтобы включить учет трафика на нескольких интерфейсах, необходимо создать соответствующее количество узлов конфигурации interface.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет настроить запись статистических данных о сетевых потоках на интерфейсе.

Форма **set** данной команды используется для включения учета входящего трафика на интерфейсе.

Форма **delete** данной команды используется для отключения учета входящего трафика на интерфейсе.

Форма **show** данной команды используется для отображения интерфейсов, на которых ведется учет трафика.

15.2.3 service flow-accounting netflow engine-id <идентификатор>

Указание идентификатора системы, который будет включен в данные NetFlow.

Синтаксис

```
set service flow-accounting netflow engine-id <идентификатор>
delete service flow-accounting netflow engine-id
show service flow-accounting netflow engine-id
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    flow-accounting {
        netflow {
            engine-id идентификатор
        }
    }
}
```

Параметры

идентификатор

Идентификатор системы, который указывается в данных NetFlow, позволяющий идентифицировать маршрутизатор, отправивший отчет. Значение должно лежать в диапазоне 0-255.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет настроить идентификатор системы, который будет указан в данных NetFlow.

Форма **set** данной команды используется для настройки идентификатора системы, который указывается в данных NetFlow.

Форма **delete** данной команды используется для удаления конфигурации идентификатора системы.

Форма **show** данной команды используется для отображения конфигурации идентификатора системы.

15.2.4 service flow-accounting netflow max-flows <количество_потоков>

Указание максимального количества потоков, отслеживаемых одновременно.

Синтаксис

```
set service flow-accounting netflow max-flows <количество_потоков>
delete service flow-accounting netflow max-flows
show service flow-accounting netflow max-flows
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   flow-accounting {
      netflow {
         max-flows количество_потоков
      }
   }
}
```

Параметры

количество_потоков

Задает максимальное количество потоков системы NetFlow. Значение должно лежать в диапазоне 1-2147483647.

Значение по умолчанию

По умолчанию установлено значение 8192.

Указания по использованию

Данная команда позволяет настроить максимальное количество потоков системы NetFlow, отслеживаемых одновременно.

Форма **set** данной команды используется для настройки количества потоков системы NetFlow.

Форма **delete** данной команды используется для удаления конфигурации количества потоков системы NetFlow.

Форма **show** данной команды используется для отображения конфигурации количества потоков системы NetFlow.

15.2.5 service flow-accounting netflow sampling-rate <частота_выборки>

Указание частоты регистрации событий для NetFlow, с которой сетевые пакеты будут учитываться в статистике.

Синтаксис

```
set service flow-accounting netflow sampling-rate <частота_выборки>
delete service flow-accounting netflow sampling-rate
show service flow-accounting netflow sampling-rate
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    flow-accounting {
        netflow {
            sampling-rate частота_выборки
        }
    }
}
```

Параметры

частота_выборки

Частота, с которой будут отбираться пакеты. Значение должно лежать в диапазоне 0-4294967295.

Значение по умолчанию

Учитываются все пакеты (то есть, значение частоты 1).

Указания по использованию

Данная команда позволяет указать частоту выборки NetFlow. Будет учитываться каждый n-ный пакет, где n - значение **sampling-rate**, настроенное для узла.

Преимущество выборки каждого n-ного пакета, где n > 1, заключается в снижении вычислительных ресурсов, требуемых для учета трафика. К недостаткам относится то, что в этом случае статистические данные будут приблизительными.

Форма **set** данной команды используется для указания частоты выборки NetFlow.

Форма **delete** данной команды используется для удаления конфигурации частоты выборки NetFlow и восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения конфигурации частоты выборки NetFlow.

15.2.6 service flow-accounting netflow server <адрес>

Указание сервера сбора данных об учете трафика (коллектора) для экспорта данных NetFlow.

Синтаксис

```
set service flow-accounting netflow server <адрес> [port <порт>]
delete service flow-accounting netflow server <адрес> [port]
show service flow-accounting netflow server <адрес> [port]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    flow-accounting {
        netflow {
            server адрес {
```

```
            port порт
        }
    }
}
```

Параметры

адрес

Множественный узел. Указание IPv4-адреса коллектора для экспорта данных NetFlow. Для того чтобы настроить экспорт на несколько удаленных серверов, следует создать соответствующее количество узлов конфигурации.

порт

Порт, на котором коллектор NetFlow принимает отчеты. По умолчанию используется порт 2055. Значение должно лежать в диапазоне 1025-65535.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать коллектор, на который будут экспортироваться данные NetFlow.

Форма **set** данной команды используется для указания коллектора NetFlow.

Форма **delete** данной команды используется для удаления конфигурации коллектора NetFlow.

Форма **show** данной команды используется для отображения конфигурации коллектора NetFlow.

15.2.7 service flow-accounting netflow timeout expiry-interval <интервал>

Указание интервала, через который будут отправляться отчеты коллектору данных NetFlow.

Синтаксис

```
set service flow-accounting netflow timeout expiry-interval <интервал>
delete service flow-accounting netflow timeout expiry-interval
show service flow-accounting netflow timeout expiry-interval
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    flow-accounting {
        netflow {
            timeout {
                expiry-interval интервал
            }
        }
    }
}
```

Параметры

интервал

Интервал времени, в секундах, через который будут отправляться отчеты коллектору NetFlow. Значение должно лежать в диапазоне 0-2147483647.

Значение по умолчанию

По умолчанию отчеты отправляются каждые 60 секунд.

Указания по использованию

Данная команда позволяет указать интервал времени, через который на удаленный коллектор NetFlow будут отправляться данные учета трафика. Предварительно должен быть определен адрес сервера NetFlow при помощи команды *system flow-accounting netflow server <адрес>*.

Форма **set** данной команды используется для указания интервала времени отправки отчетов.

Форма **delete** данной команды используется для удаления конфигурации и восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения конфигурации интервала времени отправки отчетов.

15.2.8 service flow-accounting netflow timeout flow-generic <таймаут>

Указание таймаута сетевого потока для трафика IP.

Синтаксис

```
set service flow-accounting netflow timeout flow-generic <таймаут>
delete service flow-accounting netflow timeout flow-generic
show service flow-accounting netflow timeout flow-generic
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    flow-accounting {
        netflow {
            timeout {
                flow-generic таймаут
            }
        }
    }
}
```

Параметры

таймаут

Таймаут для сетевого потока, в секундах, для общего трафика IP. Действует для трафика IP за исключением трафика протоколов TCP, UDP и ICMP. Значение должно лежать в диапазоне 1-2147483647.

Значение по умолчанию

Сетевые потоки, относящиеся к общему трафику IP, считаются завершенными по истечению 3600 секунд (1 часа).

Указания по использованию

Данная команда позволяет указать таймаут для сетевых потоков общего трафика IP. Под общим трафиком IP понимается весь трафик IP за исключением трафика протоколов TCP, UDP и ICMP. (То есть, в общий трафик IP будут включены, например, GRE, AH, ESP, и т.д.)

Данный параметр определяет интервал времени, в течение которого ожидается трафик для сетевого потока, перед тем как он станет считаться завершенным.

Форма **set** данной команды используется для указания таймаута сетевого потока для общего трафика IP.

Форма **delete** данной команды используется для восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки.

15.2.9 service flow-accounting netflow timeout icmp <таймаут>

Указание таймаута сетевого потока для трафика ICMP.

Синтаксис

```
set service flow-accounting netflow timeout icmp <таймаут>
delete service flow-accounting netflow timeout icmp
show service flow-accounting netflow timeout icmp
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   flow-accounting {
      netflow {
         timeout {
            icmp таймаут
         }
      }
   }
}
```

Параметры

таймаут

Таймаут сетевого потока, в секундах, для трафика ICMP. Значение должно лежать в диапазоне 0-2147483647.

Значение по умолчанию

Для сетевых потоков трафика ICMP установлен таймаут 300 секунд (5 минут).

Указания по использованию

Данная команда позволяет указать таймаут для сетевых потоков трафика ICMP. Данный параметр определяет интервал времени, в течение которого ожидается трафик для сетевого потока ICMP, перед тем как он станет считаться завершенным.

Форма **set** данной команды используется для указания таймаута сетевого потока для трафика ICMP.

Форма **delete** данной команды используется для восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения конфигурации таймаута для потоков ICMP.

15.2.10 service flow-accounting netflow timeout max-active-life <время_жизни>

Указание максимального интервала времени, в течении которого будет учитываться трафик, относящийся к сетевому потоку.

Синтаксис

```
set service flow-accounting netflow timeout max-active-life <время_жизни>
delete service flow-accounting netflow timeout max-active-life
show service flow-accounting netflow timeout max-active-life
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
```

```
    flow-accounting {
        netflow {
            timeout {
                max=active=life время_жизни
            }
        }
    }
}
```

Параметры

время_жизни

Интервал времени, в секундах, определяющий максимальное время учета трафика, относящегося к сетевому потоку любого типа. Значение должно лежать в диапазоне 0-2147483647.

Значение по умолчанию

Сетевые потоки любого типа считаются завершенными по истечении 604800 секунд (7 дней).

Указания по использованию

Данная команда позволяет настроить глобальное время время жизни для сетевого потока.

Данный параметр определяет интервал времени, в течение которого ожидается трафик для сетевого потока, перед тем как он станет считаться завершенным. Даже в том случае если сетевой поток все еще активен при истечении данного интервала времени, он будет считаться завершенным с точки зрения системы учета сетевого трафика.

Форма **set** данной команды используется для указания общего времени жизни для сетевого потока.

Форма **delete** данной команды используется для восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения конфигурации.

15.2.11 service flow-accounting netflow timeout tcp-fin <таймаут>

Указание таймаута сетевого потока TCP после получения пакета TCP с флагом FIN.

Синтаксис

```
set service flow-accounting netflow timeout tcp-fin <таймаут>
delete service flow-accounting netflow timeout tcp-fin
show service flow-accounting netflow timeout tcp-fin
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    flow-accounting {
        netflow {
            timeout {
                tcp-fin таймаут
            }
        }
    }
}
```

Параметры

таймаут

Таймаут сетевого потока, в секундах, после получения пакета TCP с флагом FIN. Значение должно лежать в диапазоне 0-2147483647.

Значение по умолчанию

Сетевой поток TCP считается завершенным с точки зрения системы учета трафика через 300 секунд (5 минут) после получения пакета TCP с флагом FIN (без получения последовательности пакетов с флагами FIN ACK, ACK).

Указания по использованию

Данная команда позволяет задать интервал времени, по истечении которого, после получения пакета TCP с флагом FIN, сетевой поток TCP будет считаться завершенным.

Данный параметр определяет интервал времени, в течение которого ожидается трафик для сетевого потока TCP после получения пакета TCP с флагом FIN, перед тем как он станет считаться завершенным с точки зрения системы учета трафика.

Форма **set** данной команды используется для установки таймаута.

Форма **delete** данной команды используется для восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения конфигурации.

15.2.12 service flow-accounting netflow timeout tcp-generic <таймаут>

Указание таймаута сетевого потока TCP.

Синтаксис

```
set service flow-accounting netflow timeout tcp-generic <таймаут>
delete service flow-accounting netflow timeout tcp-generic
show service flow-accounting netflow timeout tcp-generic
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   flow-accounting {
      netflow {
         timeout {
            tcp-generic таймаут
         }
      }
   }
}
```

Параметры

таймаут

Таймаут для потока TCP, в секундах. Значение должно лежать в диапазоне 0-2147483647.

Значение по умолчанию

По умолчанию установлено значение 3600 секунд. Если в течении 3600 секунд (1 часа) не будет получено трафика, относящегося к сетевому потоку, или последовательности пакетов TCP с флагами FIN, FIN ACK, ACK, сетевой поток считается завершенным с точки зрения системы учета трафика.

Указания по использованию

Данная команда позволяет указать интервал времени, по истечении которого при отсутствии трафика, относящегося к сетевому потоку, или последовательности пакетов TCP с флагами FIN, FIN ACK, ACK, сетевой поток считается завершенным с точки зрения системы учета трафика. Данный параметр определяет интервал времени, в течение которого ожидается трафик для сетевого потока или пакет TCP FIN с соответствующей последовательностью пакетов FIN ACK, ACK, перед тем как поток станет считаться завершенным.

Форма **set** данной команды используется для установки значения для таймаута.

Форма **delete** данной команды используется для восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения конфигурации.

15.2.13 service flow-accounting netflow timeout tcp-rst <таймаут>

Указание таймаута сетевого потока TCP после получения пакета TCP с флагом RST.

Синтаксис

```
set service flow-accounting netflow timeout tcp-rst <таймаут>
delete service flow-accounting netflow timeout tcp-rst
show service flow-accounting netflow timeout tcp-rst
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   flow-accounting {
      netflow {
         timeout {
            tcp-rst таймаут
         }
      }
   }
}
```

Параметры

таймаут

Таймаут сетевого потока, в секундах, после получения пакета TCP RST. Значение должно лежать в диапазоне 0-2147483647.

Значение по умолчанию

По умолчанию установлено значение 120 секунд (2 минуты). Сетевой поток TCP считается завершенным с точки зрения системы учета трафика через 120 секунд после получения пакета TCP с флагом RST (без получения последовательности пакетов с флагами TCP FIN, FIN ACK, ACK).

Указания по использованию

Данная команда позволяет задать интервал времени, по истечении которого, после получения пакетов TCP с флагом RST и отсутствии пакетов TCP FIN, FIN ACK или ACK, сетевой поток TCP будет считаться завершенным. Этот параметр определяет интервал времени, в течение которого ожидается трафик, относящийся к сетевому потоку после получения пакета TCP RST при отсутствии TCP FIN, FIN ACK, ACK, перед тем как поток станет считаться завершенным с точки зрения системы учета трафика.

Форма **set** данной команды используется для установки таймаута.

Форма **delete** данной команды используется для восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения конфигурации.

15.2.14 service flow-accounting netflow timeout udp <таймаут>

Указание таймаута сетевого потока для трафика UDP.

Синтаксис

```
set service flow-accounting netflow timeout udp <таймаут>
delete service flow-accounting netflow timeout udp
show service flow-accounting netflow timeout udp
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   flow-accounting {
      netflow {
         timeout {
            udp таймаут
         }
      }
   }
}
```

Параметры

таймаут

Таймаут сетевого потока для трафика UDP, в секундах. Значение должно лежать в диапазоне 0-2147483647.

Значение по умолчанию

Для сетевого потока трафика UDP установлено значение таймаута 300 секунд (5 минут).

Указания по использованию

Данная команда позволяет указать таймаут для сетевых потоков трафика UDP. Данный параметр определяет интервал времени, в течение которого ожидается трафик для сетевого потока UDP, перед тем как он станет считаться завершенным.

Форма **set** данной команды используется для установки таймаута сетевого потока для трафика UDP.

Форма **delete** данной команды используется для восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения конфигурации.

15.2.15 service flow-accounting netflow version <версия>

Указание формата NetFlow, в котором будут экспортированы данные учета.

Синтаксис

```
set service flow-accounting netflow version <версия>
delete service flow-accounting netflow version
show service flow-accounting netflow version
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   flow-accounting {
      netflow {
```

```
            version версия
        }
    }
}
```

Параметры

версия

Номер версии NetFlow, в формате которой будут экспортированы данные учета. Допустимые значения: 1, 5, 9.

Значение по умолчанию

По умолчанию используется версия NetFlow 5.

Указания по использованию

Данная команда позволяет указать в формате какой версии NetFlow будут экспортироваться данные учета.

Форма **set** данной команды используется для указания версии NetFlow.

Форма **delete** данной команды используется для удаления текущей конфигурации и восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения конфигурации версии NetFlow.

15.2.16 service flow-accounting sflow agent-address <адрес>

Указание IP-адреса агента sFlow.

Синтаксис

```
set service flow-accounting sflow agent-address <адрес>
delete service flow-accounting sflow agent-address
show service flow-accounting sflow agent-address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    flow-accounting {
        sflow {
            agent-address адрес
        }
    }
}
```

Параметры

адрес

IP-адрес агента sFlow, который будет указан в пакетах, отправляемых коллектору sFlow. Поддерживаются следующие значения:

auto: В этом случае автоматически выбирается IP-адрес одного из настроенных интерфейсов)

<x.x.x.x>: IPv4-адрес.

Значение по умолчанию

По умолчанию установлено значение **auto**. В качестве адреса отправителя для данных sFlow автоматически выбирается IP-адрес одного из интерфейсов, настроенных в системе.

Указания по использованию

Данная команда позволяет указать IP-адрес отправляемых коллектору sFlow данных для идентификации источника - локального Numa Edge.

Форма **set** данной команды используется для установки адреса агента.

Форма **delete** данной команды используется для удаления текущей конфигурации адреса и восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения конфигурации.

15.2.17 service flow-accounting sflow sampling-rate <частота_выборки>

Указание частоты выборки для статистики sFlow.

Синтаксис

```
set service flow-accounting sflow sampling-rate <частота_выборки>
delete service flow-accounting sflow sampling-rate
show service flow-accounting sflow sampling-rate
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   flow-accounting {
      sflow {
         sampling-rate частота-выборки
      }
   }
}
```

Параметры

частота-выборки

Частота, с которой будут отбираться пакеты. Значение должно лежать в диапазоне 0-4294967295.

Значение по умолчанию

Учитываются все пакеты (то есть, значение частоты выборки 1).

Указания по использованию

Данная команда позволяет установить частоту выборки для системы учета трафика. При установке значения n для узла **sampling-rate**, системой учета трафика будет выбран каждый n-ный пакет, который попадет в статистику.

Преимущества учета каждого n-ного пакета, где n > 1, заключается в снижении потребляемых вычислительных ресурсов, требуемых для учета трафика. К недостаткам относится то, что в этом случае статистические данные будут приблизительными.

Форма **set** данной команды используется для указания частоты выборки.

Форма **delete** данной команды используется для удаления конфигурации и восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения конфигурации.

15.2.18 service flow-accounting sflow server <адрес>

Указание адреса коллектора sFlow для экспорта данных учета.

Синтаксис

```
set service flow-accounting sflow server <адрес> [port <порт>]
```

```
delete service flow-accounting sflow server <адрес> [port]
show service flow-accounting sflow server <адрес> [port]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   flow-accounting {
      sflow {
         server адрес {
            port порт
         }
      }
   }
}
```

Параметры

адрес

Множественный узел. IPv4-адрес коллектора sFlow для экспорта учетных данных. Для того чтобы настроить экспорт на несколько удаленных серверов, следует создать соответствующее количество узлов конфигурации.

порт

Формат – целоебеззнака [1025-65535]. Порт, на котором коллектор sFlow принимает отчеты. По умолчанию используется порт 6343. Значение должно лежать в диапазоне 1025-65535.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать коллектор sFlow, на который будут экспортироваться данные учета.

Форма **set** данной команды используется для указания коллектора sFlow.

Форма **delete** данной команды используется для удаления текущей конфигурации и восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения конфигурации коллекора sFlow.

15.2.19 service flow-accounting syslog-facility <источник>

Указание типов сообщений, относящихся к учету трафика, которые будут регистрироваться в журнале.

Синтаксис

```
set service flow-accounting syslog-facility <источник>
delete service flow-accounting syslog-facility
show service flow-accounting syslog-facility
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
  flow-accounting {
      syslog-facility источник
   }
```

```
}
```

Параметры

источник

Источник сообщений, от имени которого сообщения, связанные с учетом трафика, будут регистрироваться в журнале. Подробнее, источники сообщений рассмотрены в разделе **Регистрация**.

Значение по умолчанию

По умолчанию используется источник сообщений **daemon**.

Указания по использованию

Данная команда позволяет указать тип источника для сообщений, относящихся к учету трафика, которые будут регистрироваться в журнале.

Форма **set** данной команды используется для указания источника сообщений, связанных с учетом трафика, от имени которого они будут зарегистрированы в журнале.

Форма **delete** данной команды используется для удаления текущей конфигурации и восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения конфигурации регистрационных сообщений, связанных с учетом сетевого трафика.

15.2.20 service flow-accounting clear counters

Очистка всех счетчиков учета трафика.

Синтаксис

```
service flow-accounting clear counters
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет очистить счетчики учета трафика на всех настроенных интерфейсах.

15.2.21 service flow-accounting show

Отображение статистики потока для всех(указанного) интерфейсов(-а), на которых(-ом) ведется учет трафика.

Синтаксис

```
service flow-accounting show [interface <интерфейс> [host <адрес> | port
<порт> | top <количество_потоков>]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

интерфейс

Наименование интерфейса в системе, для которого необходимо отобразить статистику сетевого трафика.

адрес

IPv4-адрес, по которому будут отфильтрованы данные статистики сетевого трафика.

порт

Номер сетевого порта, по которому будут отфильтрованы данные статистики сетевого трафика. Значение должно лежать в диапазоне 1-65535.

количество_потоков

Количество потоков с наибольшим трафиком, по которым будут выведены данные статистики сетевого трафика. Отображаются в порядке убывания в зависимости от количества байтов, полученных на интерфейсе. Значение должно лежать в диапазоне 1-65535.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет отобразить статистические данные о сетевом трафике, собранные системой учета сетевого трафика. По умолчанию будут выведены все собранные данные о сетевом трафике для всех сетевых интерфейсов, на которых ведется учет трафика. При указании в команде определенного интерфейса будет выведена статистика только по указанному интерфейсу. С помощью параметров **host** и **port** можно дополнительно отфильтровать собранную статистику по интересующим IP-адресам и портам. С помощью параметра **top** можно вывести определенной количество потоков с наибольшим трафиком.

15.2.22 service flow-accounting restart

Перезапуск процесса системы учета сетевого трафика.

Синтаксис

```
service flow-accounting restart
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда предназначена для перезапуска работающего процесса системы учета сетевого трафика.

16 Фильтры трафика

16.1 Функциональность фильтров трафика системы Numa Edge

Механизм фильтров трафика предназначен для выборки требуемых пакетов по критериям, определённым фильтром. Заданный фильтр сам по себе никак не влияет на обрабатываемый устройством трафик, однако может использоваться при задании политик маршрутизации, QoS и модификации трафика.

16.1.1 Определение фильтров трафика

Фильтр трафика представляет собой именованный упорядоченный набор правил отбора. Каждое правило содержит набор критериев, с которым сравнивается обрабатываемый пакет, соответствие всем критериям правила означает, что пакет удовлетворяет заданному фильтру. Так как правила фильтра упорядочены, проверка соответствия пакета заданным правилам производится в порядке нумерации правил. Это особенно важно при использовании правил исключения из фильтра, пакет удовлетворяющий критериям такого правила будет считаться не соответствующим заданному фильтру и проверка по дальнейшим определённым фильтром правилам проводиться не будет.

16.1.2 Примеры настройки фильтров трафика

В данном разделе приведены примеры настройки фильтров трафика. Рассматриваются следующие вопросы:

- пример настройки фильтра трафика с двумя правилами;
- пример настройки фильтра трафика с правилом исключения.

Пример настройки фильтра трафика с двумя правилами

В примере показана настройка фильтра на определение трафика, идущего на указанные IP-адреса по протоколам HTTP, HTTPS и FTP из определенной подсети. Данные протоколы базируются на транспортном протоколе TCP и используют стандартные порты для установки как открытых, так и защищенных (SSL/TLS) соединений. В дальнейшем этот фильтр может быть использован в рамках реализации политик QoS для приоритизации трафика при распределении пропускной способности канала, а также рамках реализации политик маршрутизации, модификации и клонирования трафика. При этом возможно использование фильтра как во всех политиках одновременно, так и в рамках реализации одной конкретной политики.

Для выполнения данной настройки создаётся фильтр трафика Server с двумя определёнными правилами:

- правило номер 10 настроено на определение пакетов, приходящих от IP-адресов из подсети 192.168.10.0/24;
- правило номер 20 настроено на определение пакетов, направляемых на IP-адреса 192.168.20.10-192.168.20.12 и порты номер 80, 443 и 21 (при создании правила используются имена http,https и ftp, соответствующие данным портам) по протоколу TCP.

При такой настройке трафик соответствует критериям фильтра, при соответствии всем критериям, указанным в одном из правил.

Для выполнения данной настройки необходимо выполнить следующую последовательность команд в режиме настройки.

Пример 131– Настройка фильтра трафика с двумя правилами

Действие	**Команда**
Создание фильтра трафика с именем Server и указание его описания	`[edit]` `admin@edge# set filter Server description "Server traffic filter"`
Указание текстового описания для правила определения адреса источника	`[edit]` `admin@edge# set filter Server rule 10 description "Source address"`
Указание подсети 192.168.10.0/24 в качестве адресов источника поступления данных в рамках данного правила	`[edit]` `admin@edge# set filter Server rule 10 source address 192.168.10.0/24`
Указание текстового описания для правила	`[edit]`

Действие	Команда
определения адреса и порта получателя	admin@edge# set filter Server rule 20 description "Destination address and port"
Указание TCP в качестве протокола, пакеты которого должны определяться в рамках данного правила	[edit] admin@edge# set filter Server rule 20 protocol tcp
Указание диапазона адресов 192.168.20.10-192.168.20.12 в качестве адресов назначения для отправки данных в рамках данного правила	[edit] admin@edge# set filter Server rule 20 destination address 192.168.20.10-192.168.20.12
Указание портов http,https,ftp (порты номер 80, 443 и 21) в качестве портов назначения для отправки данных в рамках данного правила	[edit] admin@edge# set filter Server rule 20 destination port http,https,ftp
Фиксация настройки	[edit] admin@edge# commit

Отображение настройки	[edit]
	admin@edge# show filter
	Server {
	description "Server traffic filter"
	rule 10 {
	description "Source address"
	source {
	address 192.168.10.0/24
	}
	}
	rule 20 {
	description "Destination address and port"
	destination {
	address 192.168.20.10-192.168.20.12
	port http,https,ftp
	}
	protocol tcp
	}
	}

Пример настройки фильтра трафика с правилом исключения

В примере выполняется настройка фильтра трафика с именем ICMP с применением правила исключения. Первое правило является правилом исключения. Оно настроено на исключение пакетов, приходящих с IP-адреса 192.168.10.20 по протоколу ICMP. Второе правило настроено на определение пакетов, приходящих из подсети 192.168.10.0/24 по протоколу ICMP. При такой настройке, трафик проверяется на соответствие критериям правил в порядке нумерации. Трафик считается соответствующим критериям фильтра, если он соответствует критериям второго правила и не соответствует критериям первого.

Для выполнения данной настройки необходимо выполнить следующую последовательность команд в режиме настройки.

Пример 132– Настройка фильтра трафика с правилом исключения

Действие	Команда
Создание фильтра трафика с именем ICMP и указание его описания	[edit] admin@edge# set filter ICMP description "ICMP 192.168.10.0/24 exclude 192.168.10.20"
Указание адреса отправителя трафика для дальнейшего исключения его из диапазона. В качестве отправителя указывается IP-адрес 192.168.10.20	[edit] admin@edge# set filter ICMP rule 10 source address 192.168.10.20
Указание ICMP в качестве протокола, пакеты которого	[edit]

Действие	Команда
должны определяться в рамках данного правила	`admin@edge# set filter ICMP rule 10 protocol icmp`
Указание параметра исключения пакетов, удовлетворяющих критериям правила фильтрации трафика, из фильтра	`[edit]` `admin@edge# set filter ICMP rule 10 exclude`
Указание ICMP в качестве протокола, пакеты которого должны определяться в рамках данного правила	`[edit]` `admin@edge# set filter ICMP rule 20 protocol icmp`
Указание адреса отправителя трафика. В качестве отправителя указывается подсеть 192.168.10.0/24	`[edit]` `admin@edge# set filter ICMP rule 20 source address 192.168.10.0/24`
Фиксация настройки	`[edit]` `admin@edge# commit`

Отображение настройки	`[edit]`
	`admin@edge# show filter`
	`ICMP {`
	`description "ICMP 192.168.10.0/24 exclude 192.168.10.20"`
	`rule 10 {`
	`exclude`
	`protocol icmp`
	`source {`
	`address 192.168.10.20`
	`}`
	`}`
	`rule 20 {`
	`protocol icmp`
	`source {`
	`address 192.168.10.0/24`
	`}`
	`}`
	`}`

16.2 Команды настройки фильтров трафика

В данном разделе приведены команды для настройки фильтров трафика.

Режим настройки	
Фильтры трафика IPv4	
filter <имя>	Указание имени фильтра трафика IPv4.
filter <имя> description <описание>	Указание краткого описания для фильтра трафика IPv4.
filter <имя> rule <номер_правила>	Определение правила указанного фильтра трафика IPv4.
filter <имя> rule <номер_правила> 32bits	Сопоставление 32-битных слов внутри пакета.
filter <имя> rule <номер_правила> 32bits invert	Инверсия сопоставления 32-битных слов внутри пакета.
filter <имя> rule <номер_правила> 32bits match <параметр_сопоставления> location <адрес>	Задание адреса и преобразования значения сопоставления 32-битных слов внутри пакета.
filter <имя> rule <номер_правила> 32bits match <параметр_сопоставления> value <значение>	Задание значения для сопоставления 32-битных слов внутри пакета.
filter <имя> rule <номер_правила> description <описание>	Указание краткого описания для правила фильтрации трафика IPv4.
filter <имя> rule <номер_правила> destination address <адрес>	Указание адреса получателя для проверки соответствия в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> destination address-group <имя_группы>	Указание группы адресов для проверки соответствия IP-адреса получателя сетевого пакета в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> destination	Указание типа адреса получателя, по которому будет

address-type <тип>	осуществляться проверка соответствия в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> destination country <код_страны>	Указание двухзначного кода страны получателя в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> destination domain-group <имя_группы>	Указание группы доменов для проверки соответствия домена получателя сетевого пакета в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> destination ldap	Указание имени пользователя и(или) группы LDAP для проверки соответствия в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> destination network-group <имя_группы>	Указание группы сетей для проверки соответствия IP-адреса сети получателя сетевого пакета в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> destination port <порт>	Указание номера сетевого порта получателя для проверки соответствия в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> destination port-group <имя_группы>	Указание группы портов для проверки соответствия порта получателя сетевого пакета в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> disable	Отключение указанного правила фильтрации трафика IPv4.
filter <имя> rule <номер_правила> dscp <значение>	Установка соответствия на основе поля DSCP.
filter <имя> rule <номер_правила> ecn ip ect <значение>	Установка соответствия на основе флага ECT в заголовке IP.
filter <имя> rule <номер_правила> ecn tcp cwr <значение>	Установка соответствия на основе флага CWR в заголовке TCP.
filter <имя> rule <номер_правила> ecn tcp ece <значение>	Установка соответствия на основе флага ECE в заголовке TCP.
filter <имя> rule <номер_правила> exclude	Исключение правила из фильтра.
filter <имя> rule <номер_правила> fragment <тип>	Указание типа проверки соответствия для фрагментированных пакетов.
filter <имя> rule <номер_правила> icmp type <тип>	Указание кода и типа ICMP для правила фильтрации трафика IPv4.
filter <имя> rule <номер_правила> ipsec <тип>	Установка соответствия для пакетов IPSec.
filter <имя> rule <номер_правила> ipv4options mode <режим>	Установка режима для критерия соответствия на основе поля опций в заголовке IPv4-пакета.
filter <имя> rule <номер_правила> ipv4options opts <список_опций>	Указание списка опций IP, которые будут использоваться в критерии соответствия на основе поля опций в заголовке IP-пакета.
filter <имя> rule <номер_правила> l7protocol <протокол>	Указание протокола для фильтрации пакетов на прикладном уровне.
filter <имя> rule <номер_правила> length	Указание параметров, ограничивающих длину пакетов для правила фильтрации трафика IPv4.
filter <имя> rule <номер_правила> limit connection-rate	Указание параметров, ограничивающих частоту прохождения пакетов для соединения в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> limit connections	Указание параметров, ограничивающих количество соединений в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> limit packet-rate	Указание параметров, ограничивающих частоту прохождения пакетов в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> log <состояние>	Включение или отключение регистрации для действий правила фильтрации трафика IPv4.
filter <имя> rule <номер_правила> p2p <имя_приложения>	Указание одноранговое приложения для фильтрации его IPv4-пакетов на прикладном уровне.

filter <имя> rule <номер_правила> probability <вероятность>	Указание вероятности срабатывания правила в процентах.
filter <имя> rule <номер_правила> protocol <протокол>	Указание протокола для фильтрации пакетов.
filter <имя> rule <номер_правила> quota overall	Настройка квотирования фильтрации пакетов по всему объёму данных или числу пакетов.
filter <имя> rule <номер_правила> quota per-connection	Настройка квотирования фильтрации пакетов по объёму данных или числу пакетов на соединение.
filter <имя> rule <номер_правила> recent	Установка соответствия для сетевых пакетов от недавно встречавшихся отправителей.
filter <имя> rule <номер_правила> sctp chunk-type	Установка параметров протокола SCTP для проверки соответствия в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> source address <адрес>	Указание адреса отправителя для проверки соответствия в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> source address-group <имя_группы>	Указание группы адресов для проверки соответствия IP-адреса отправителя сетевого пакета в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> source address-type <тип>	Указание типа адреса отправителя, по которому будет осуществляться проверка соответствия в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> source country <код_страны>	Указание двухзначного кода страны отправителя в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> source domain-group <имя_группы>	Указание группы доменов для проверки соответствия домена отправителя сетевого пакета в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> source ldap	Указание имени пользователя и(или) группы LDAP для проверки соответствия в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> source local-group <имя_группы>	Указание локальной группы МЭ для проверки соответствия в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> source local-user <имя_пользователя>	Указание локального пользователя МЭ для проверки соответствия в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> source mac-address <mac-адрес>	Указание MAC-адреса отправителя, по которому будет осуществляться проверка соответствия в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> source network-group <имя_группы>	Указание группы сетей для проверки соответствия IP-адреса сети отправителя сетевого пакета в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> source port <порт>	Указание номера сетевого порта для проверки соответствия в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> source port-group <имя_группы>	Указание группы портов для проверки соответствия порта отправителя сетевого пакета в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> state	Указание состояний соединений, к которым применяется правило фильтрации трафика IPv4.
filter <имя> rule <номер_правила> string <номер_подстроки> case-insensitive	Не учитывать регистр букв при фильтрации по подстрокам в IPv4-пакете.
filter <имя> rule <номер_правила> string <номер_подстроки> from <смещение>	Установка смещения в пакете IPv4, начиная с которого будет осуществляться поиск подстроки.
filter <имя> rule <номер_правила> string <номер_подстроки> hex-match <подстрока>	Указание подстроки для поиска в шестнадцатеричном виде.
filter <имя> rule <номер_правила> string <номер_подстроки> match <подстрока>	Указание подстроки для поиска.
filter <имя> rule <номер_правила> string	Установка соответствия на основе отсутствия указанной

<номер_подстроки> negation	подстроки в пакете IPv4.
filter <имя> rule <номер_правила> string <номер_подстроки> to <смещение>	Установка смещения в пакете IPv4, до которого будет осуществляться поиск подстроки.
filter <имя> rule <номер_правила> tcp flags <флаг>	Указание флагов TCP для проверки соответствия в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> tcp mss <значение>	Указание максимального размера сегмента для проверки соответствия в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> tcp option <опция>	Указание опции TCP для проверки соответствия в правиле фильтрации трафика IPv4.
filter <имя> rule <номер_правила> time	Применение правил фильтрации трафика с учетом даты и времени.
filter <имя> rule <номер_правила> ttl <значение>	Применение правил фильтрации трафика с учетом времени жизни пакетов.
Фильтры трафика IPv6	
filter-ipv6 <имя>	Указание имени фильтра трафика IPv6.
filter-ipv6 <имя> description <описание>	Указание краткого описания для фильтра трафика IPv6.
filter-ipv6 <имя> rule <номер_правила>	Определение правила указанного фильтра трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> 32bits	Сопоставление 32-битных слов внутри пакета.
filter-ipv6 <имя> rule <номер_правила> 32bits invert	Инверсия сопоставления 32-битных слов внутри пакета.
filter-ipv6 <имя> rule <номер_правила> 32bits match <параметр_сопоставления> location <адрес>	Задание адреса и преобразования значения сопоставления 32-битных слов внутри пакета.
filter-ipv6 <имя> rule <номер_правила> 32bits match <параметр_сопоставления> value <значение>	Задание значения для сопоставления 32-битных слов внутри пакета.
filter-ipv6 <имя> rule <номер_правила> description <описание>	Указание краткого описания для правила фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> destination address <адрес>	Указание адреса получателя для проверки соответствия в правиле фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> destination address-type <тип>	Указание типа адреса получателя, по которому будет осуществляться проверка соответствия в правиле фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> destination country <код_страны>	Указание двухзначного кода страны получателя в правиле фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> destination port <порт>	Указание номера сетевого порта получателя для проверки соответствия в правиле фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> disable	Отключение указанного правила фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> dscp <значение>	Установка соответствия на основе поля DSCP.
filter-ipv6 <имя> rule <номер_правила> ecn ip ect <значение>	Установка соответствия на основе флага ECT в заголовке IP.
filter-ipv6 <имя> rule <номер_правила> ecn tcp cwr <значение>	Установка соответствия на основе флага CWR в заголовке TCP.
filter-ipv6 <имя> rule <номер_правила> ecn tcp ece <значение>	Установка соответствия на основе флага ECE в заголовке TCP.
filter-ipv6 <имя> rule <номер_правила> exclude	Исключение правила из фильтра.
filter-ipv6 <имя> rule <номер_правила> hop-limit <значение>	Применение правил фильтрации трафика с учетом ограничения транзитных узлов.
filter-ipv6 <имя> rule <номер_правила> icmpv6 type <тип>	Указание кода и типа ICMPv6 для правила фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> ipsec <тип>	Установка соответствия для пакетов IPSec.
filter-ipv6 <имя> rule <номер_правила> l7protocol <протокол>	Указание протокола для фильтрации пакетов на прикладном уровне.

filter-ipv6 <имя> rule <номер_правила> length	Указание параметров, ограничивающих длину пакетов для правила фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> limit connection-rate	Указание параметров, ограничивающих частоту прохождения пакетов для соединения в правиле фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> limit connections	Указание параметров, ограничивающих количество соединений в правиле фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> limit packet-rate	Указание параметров, ограничивающих частоту прохождения пакетов в правиле фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> log <состояние>	Включение или отключение регистрации для действий правила фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> p2p <имя_приложения>	Указание одноранговогo приложения для фильтрации его IPv6-пакетов на прикладном уровне.
filter-ipv6 <имя> rule <номер_правила> probability <вероятность>	Указание вероятности срабатывания правила в процентах.
filter-ipv6 <имя> rule <номер_правила> protocol <протокол>	Указание протокола для фильтрации пакетов.
filter-ipv6 <имя> rule <номер_правила> quota overall	Настройка квотирования фильтрации пакетов по всему объёму данных или числу пакетов.
filter-ipv6 <имя> rule <номер_правила> quota per-connection	Настройка квотирования фильтрации пакетов по объёму данных или числу пакетов на соединение.
filter-ipv6 <имя> rule <номер_правила> recent	Установка соответствия для сетевых пакетов от недавно встречавшихся отправителей.
filter-ipv6 <имя> rule <номер_правила> sctp chunk-type	Установка параметров протокола SCTP для проверки соответствия в правиле фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> source address <адрес>	Указание адреса отправителя для проверки соответствия в правиле фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> source address-type <тип>	Указание типа адреса отправителя, по которому будет осуществляться проверка соответствия в правиле фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> source country <код_страны>	Указание двухзначного кода страны отправителя в правиле фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> source local-group <имя_группы>	Указание локальной группы МЭ для проверки соответствия в правиле фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> source local-user <имя_пользователя>	Указание локального пользователя МЭ для проверки соответствия в правиле фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> source mac-address <mac-адрес>	Указание MAC-адреса отправителя, по которому будет осуществляться проверка соответствия в правиле фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> source port <порт>	Указание номера сетевого порта отправителя для проверки соответствия в правиле фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> state	Указание состояний соединений, к которым применяется правило фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> case-insensitive	Не учитывать регистр букв при фильтрации по подстрокам в IPv6-пакете.
filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> from <смещение>	Установка смещения в пакете IPv6, начиная с которого будет осуществляться поиск подстроки.
filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> hex-match <подстрока>	Указание подстроки для поиска в шестнадцатеричном виде.
filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> match <подстрока>	Указание подстроки для поиска.
filter-ipv6 <имя> rule <номер_правила> string	Установка соответствия на основе отсутствия указанной

<номер_подстроки> negation	подстроки в пакете IPv6.
filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> to <смещение>	Установка смещения в пакете IPv6, до которого будет осуществляться поиск подстроки.
filter-ipv6 <имя> rule <номер_правила> tcp flags <флаг>	Указание флагов TCP для проверки соответствия в правиле фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> tcp mss <значение>	Указание максимального размера сегмента для проверки соответствия в правиле фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> tcp option <опция>	Указание опции TCP для проверки соответствия в правиле фильтрации трафика IPv6.
filter-ipv6 <имя> rule <номер_правила> time	Применение правил фильтрации трафика с учетом даты и времени.

16.2.1 filter <имя>

Указание имени фильтра трафика IPv4.

Синтаксис

```
set filter <имя>
delete filter <имя>
show filter <имя>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {}
```

Параметры

имя

Имя фильтра трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать имя фильтра трафика. Следует отметить, что при создании пустого узла **filter** (без правил) трафик IPv4 им обрабатываться не будет. Настройка узла **filter** не влияет на трафик IPv6.

Форма **set** данной команды используется для указания имени фильтра трафика.

Форма **delete** данной команды используется для удаления фильтра трафика с заданным именем.

Форма **show** данной команды используется для отображения фильтра трафика.

16.2.2 filter <имя> description <описание>

Указание краткого описания для фильтра трафика IPv4.

Синтаксис

```
set filter <имя> description <описание>
delete filter <имя> description
show filter <имя> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
  description описание
```

```
}
```

Параметры

имя

Имя фильтра трафика.

описание

Описание фильтра трафика. Если текст описания фильтра трафика не содержит пробелов, то *описание* не требует использования дополнительных символов, иначе *описание* заключается либо в одинарные (*'описание'*), либо в двойные (*"описание"*) кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать описание для фильтра трафика IPv4.

Форма **set** данной команды используется для создания и изменения описания.

Форма **delete** данной команды используется для удаления описания.

Форма **show** данной команды используется для отображения настройки описания.

16.2.3 filter <имя> rule <номер_правила>

Определение правила указанного фильтра трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила>
delete filter <имя> rule <номер_правила>
show filter <имя> rule <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно находиться в диапазоне от 1 до 9999. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации **rule**.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет определить правило определённого фильтра трафика IPv4. Определённый фильтр трафика может включать в себя до 9999 настраиваемых правил.

Правила в фильтре трафика в порядке следования их номеров, от наименьшего к наибольшему. Напрямую изменить номер правила нельзя, так как он является идентификатором узла конфигурации; однако, можно изменять номера правил при помощи команды **rename**. Для того чтобы не прибегать к изменению номеров

правил, хорошей практикой является указание номеров с шагом 10. Это позволяет оставить пространство, куда можно будет впоследствии добавить новые правила.

Следует отметить, что при создании правила соответствия без уточняющих параметров, весь трафик IPv4 будет попадать под его действие.

Форма **set** данной команды используется для создания или изменения правила определённого фильтра трафика.

Форма **delete** данной команды используется для удаления правила из фильтра трафика.

Форма **show** данной команды используется для отображения настройки правила фильтра трафика.

16.2.4 filter <имя> rule <номер_правила> 32bits

Сопоставление 32-битных слов внутри пакета.

Синтаксис

```
set filter <имя> rule <номер_правила> 32bits
delete filter <имя> rule <номер_правила> 32bits
show filter <имя> rule <номер_правила> 32bits
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      32bits {
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать сопоставление 32-битных слов внутри пакета.

Форма **set** данной команды используется для создания сопоставления.

Форма **delete** данной команды используется для удаления сопоставления.

Форма **show** данной команды используется для отображения настройки сопоставления.

16.2.5 filter <имя> rule <номер_правила> 32bits invert

Инверсия сопоставления 32-битных слов внутри пакета.

Синтаксис

```
set filter <имя> rule <номер_правила> 32bits invert
delete filter <имя> rule <номер_правила> 32bits invert
show filter <имя> rule <номер_правила> 32bits
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя
   rule номер_правила {
      32bits {
         invert
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

Invert

При указании данного параметра будет осуществляться инверсия сопоставления 32-битных слов внутри пакета.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать инверсию сопоставления 32-битных слов внутри пакета.

Форма **set** данной команды используется для создания инверсии сопоставления.

Форма **delete** данной команды используется для удаления инверсии сопоставления.

Форма **show** данной команды используется для отображения настройки инверсии сопоставления.

16.2.6 filter <имя> rule <номер_правила> 32bits match <параметр_сопоставления> location <адрес>

Задание адреса и преобразования значения сопоставления 32-битных слов внутри пакета.

Синтаксис

```
set filter <имя> rule <номер_правила> 32bits match <параметр_сопоставления> location <адрес>
delete filter <имя> rule <номер_правила> 32bits match <параметр_сопоставления> location <адрес>
show filter <имя> rule <номер_правила> 32bits match <параметр_сопоставления> location
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      32bits {
        match параметр_сопоставления {
           location адрес
```

```
            }
          }
      }
  }
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

параметр_сопоставления

Параметр сопоставления. Значение должно находиться в диапазоне от 0 до 4294967295.

адрес

Адрес и преобразования значения. Поддерживаются следующие значения:

Таблица 62 - Допустимые значения поля location

Значение	**Описание**
<0-4294967295>	Десятичный адрес значения
<0x00000000-0xFFFFFFFF>	Шестнадцатеричный адрес значения
x & y	Маска *y* (битовое "и") значения *x*
x << y	Сдвиг значения *x* влево на *y*
x >> y	Сдвиг значения *x* вправо на *y*
x @ y	Использование значения по смещению *y* относительно адреса *x*

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет задать адрес и преобразование значения сопоставления 32-битных слов внутри пакета.

Форма **set** данной команды используется для задания адреса.

Форма **delete** данной команды используется для удаления адреса.

Форма **show** данной команды используется для отображения настройки адреса.

16.2.7 filter <имя> rule <номер_правила> 32bits match <параметр_сопоставления> value <значение>

Задание значения для сопоставления 32-битных слов внутри пакета.

Синтаксис

```
set filter <имя> rule <номер_правила> 32bits match <параметр_сопоставления> value <значение>

delete filter <имя> rule <номер_правила> 32bits match <параметр_сопоставления> value <значение>

show filter <имя> rule <номер_правила> 32bits match <параметр_сопоставления> value
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
```

```
    rule номер_правила {
        32bits {
            match параметр_сопоставления {
              value значение
            }
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

параметр_сопоставления

Параметр сопоставления. Значение должно находиться в диапазоне от 0 до 4294967295.

значение

Значение для сопоставления. Поддерживаются следующие значения:

Таблица 63 - Допустимые значения поля value

Значение	**Описание**
<0-4294967295>	Десятичное значение
<0x00000000-0xFFFFFFFF>	Шестнадцатеричное значение
<x-y>	Диапазон значений

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет задать значения для сопоставления 32-битных слов внутри пакета.

Форма **set** данной команды используется для задания значения.

Форма **delete** данной команды используется для удаления значения.

Форма **show** данной команды используется для отображения настройки.

16.2.8 filter <имя> rule <номер_правила> description <описание>

Указание краткого описания для правила фильтрации трафика IPv4.

Синтаксис

```
set filter <имя>rule <номер_правила> description <описание>
delete filter <имя> rule <номер_правила> description
show filter <имя> rule <номер_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
    rule номер_правила {
        description описание
```

```
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

Описание

Краткое описание правила. Если текст описания содержит пробелы, то его следует заключить в кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать краткое описание для правила фильтрации трафика определённого фильтра.

Форма **set** данной команды используется для создания описания.

Форма **delete** данной команды используется для удаления описания.

Форма **show** данной команды используется для отображения настройки описания.

16.2.9 filter <имя> rule <номер_правила> destination address <адрес>

Указание адреса получателя для проверки соответствия в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> destination address <адрес>
delete filter <имя> rule <номер_правила>destination address <адрес>
show filter <имя> rule <номер_правила> destination address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
    rule номер_правила {
        destination {
            address адрес
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

адрес

Адрес получателя, используемый для проверки соответствия. Поддерживаемые значения приведены в таблице ниже.

Таблица 64 - Поддерживаемые значения адреса получателя

Значение	Описание
<x.x.x.x>	Адрес IPv4
<x.x.x.x/x>	Подсеть IPv4 (значение 0.0.0.0/0 соответствует любой сети)
<x.x.x.x>-<x.x.x.x>	Диапазон IPv4-адресов
!<x.x.x.x>	Соответствие будет установлено для всех IPv4-адресов, кроме указанного
!<x.x.x.x/x>	Соответствие будет установлено для всех IPv4-адресов, кроме указанной подсети
!<x.x.x.x>-<x.x.x.x>	Соответствие будет установлено для всех IPv4-адресов, кроме адресов, входящих в указанный диапазон

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать адрес получателя в правиле фильтрации трафика IPv4.

В том случае если явно указаны адрес и номер порта, для пакета устанавливается соответствие критериям правила в том и только том случае, если совпадает как адрес, так и номер порта.

ПРИМЕЧАНИЕ Для указания адреса получателя адрес задается либо данной командой, либо указанием группы адресов командой filter <имя> rule <номер_правила> destination address-group <имя_группы>. Параллельное использование обоих механизмов не допускается.

Форма **set** данной команды позволяет указать или изменить адрес получателя.

Форма **delete** данной команды позволяет удалить настройку адреса получателя.

Форма **show** данной команды позволяет отобразить настройку адреса получателя.

16.2.10 filter <имя> rule <номер_правила> destination address-group <имя_группы>

Указание группы адресов для проверки соответствия IP-адреса получателя сетевого пакета в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> destination address-group <имя_группы>
delete filter <имя> rule <номер_правила> destination address-group <имя_группы>
show filter <имя> rule <номер_правила>  destination address-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
    rule номер_правила  destination {
          address-group имя_группы
       }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

имя_группы

Имя группы IPv4-адресов.

Таблица 65 - Допустимые значения для группы адресов

Значение	Описание
<text>	Имя группы
!<text>	Все группы кроме указанной

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет использовать заранее определенную группу адресов для сопоставления с IPv4-адресом получателя пакета. Группа должна быть предварительно определена при помощи команды *groups address-group <имя_группы>*. Может быть указана только одна группа.

Соответствие для пакета устанавливается в том случае, если IP-адрес совпадает с одним из адресов, входящих в состав указанной группы.

ПРИМЕЧАНИЕ Для указания адреса получателя адрес задается либо указанием группы адресов данной командой, либо указанием адресов командой filter <имя> rule <номер_правила> destination address <адрес>. Параллельное использование обоих механизмов не допускается.

Форма **set** данной команды используется для указания группы адресов получателя для проверки соответствия.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.11 filter <имя> rule <номер_правила> destination address-type <тип>

Указание типа адреса получателя, по которому будет осуществляться проверка соответствия в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> destination address-type <тип>
delete filter <имя> rule <номер_правила> destination address-type <тип>
show filter <имя> rule <номер_правила> destination address-type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      destination {
         address-type тип
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

тип

Тип адреса получателя (назначения). Данное правило будет применено к пакетам, тип адреса получателя (назначения) которых соответствует указанному. Допустимые значения приведены в таблице ниже.

Таблица 66 - Допустимые значения типа адреса получателя

Значение	**Описание**
unspec	Неопределённый адрес (0.0.0.0)
unicast	Однонаправленный адрес
local	Локальный адрес
broadcast	Широковещательный адрес
multicast	Мультивещательный адрес
anycast	Близковещательный адрес (anycast)
blackhole	Адрес подпадающий под маршрут типа "чёрная дыра"
unreachable	Недостижимый адрес
prohibit	Административно запрещённый для маршрутизации адрес
nat	Преобразуемый сетевой адрес

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать тип адреса получателя в правиле фильтрации трафика IPv4.

Форма **set** данной команды используется для создания настройки типа адреса назначения для правила фильтрации трафика.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.12 filter <имя> rule <номер_правила> destination country <код_страны>

Указание двухзначного кода страны получателя в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> destination country <код_страны>
delete filter <имя> rule <номер_правила> destination country <код_страны>
show filter <имя> rule <номер_правила> destination country
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
     destination {
         country код_страны
     }
  }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

код_страны

Двузначный код страны получателя.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания двухзначного кода страны получателя в правиле фильтрации трафика IPv4. В одном правиле фильтрации может быть задано не более 15 стран.

ПРИМЕЧАНИЕ Необходимо иметь в виду, что данные о принадлежности IP диапазона к определенному региону берутся из общедоступных источников и могут не обладать 100% точностью. Для дополнения/исключения диапазонов рекомендуется использовать группы IP адресов (groups address-group) в правилах фильтрации.

Форма **set** данной команды используется для указания двухзначного кода страны получателя в правиле фильтрации трафика.

Форма **delete** данной команды используется для удаления настройки двухзначного кода страны получателя в правиле фильтрации трафика.

Форма **show** данной команды используется для просмотра настройки двухзначного кода страны получателя в правиле фильтрации трафика.

16.2.13 filter <имя> rule <номер_правила> destination domain-group <имя_группы>

Указание группы доменов для проверки соответствия домена получателя сетевого пакета в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> destination domain-group <имя_группы>
delete filter <имя> rule <номер_правила> destination domain-group <имя_группы>
show filter <имя> rule <номер_правила> destination domain-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
    rule номер_правила {
        destination {
            domain-group имя_группы
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

имя_группы

Имя группы доменов.

Таблица 67 - Допустимые значения для группы доменов

Значение	Описание
<text>	Имя группы
!<text>	Все группы кроме указанной

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет использовать заранее определенную группу доменов для сопоставления с доменом получателя пакета. Группа должна быть предварительно определена при помощи команды *groups domain-group <имя_группы>*. Может быть указана только одна группа.

Соответствие для пакета устанавливается в том случае, если домен совпадает с одним из доменов, входящих в состав указанной группы.

Форма **set** данной команды используется для указания группы доменов получателя для проверки соответствия.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.14 filter <имя> rule <номер_правила> destination ldap

Указание имени пользователя и(или) группы LDAP для проверки соответствия в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> destination ldap [group <имя_группы> | user <имя_пользователя>]
delete filter <имя> rule <номер_правила> destination ldap [group | user]
show filter <имя> rule <номер_правила> destination ldap [group | user]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
    rule номер_правила {
        destination {
            ldap {
                group имя_группы
                user имя_пользователя
            }
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

имя_группы

Данное правило будет применено к пакетам, получателем которых являются клиент VPN PPTP/L2TP, который был аутентифицирован на основе учетной записи пользователя LDAP, входящего в указанную группу.

имя_пользователя

Данное правило будет применено к пакетам, получателем которых является клиент VPN PPTP/L2TP, который был аутентифицирован на основе учетной записи пользователя LDAP с указанным именем.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать имя пользователя и(или) группы LDAP, для тех случаев когда получателем является клиент PPTP/L2TP, который был аутентифицирован на основе учетной записи пользователя LDAP с указанным именем.

Форма **set** данной команды используется для создания настройки получателя для правила фильтрации трафика.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.15 filter <имя> rule <номер_правила> destination network-group <имя_группы>

Данный узел команд присутствует в системе для обеспечения обратной совместимости со старыми версиями оборудования. Вместо него следует использовать функционал filter <имя> rule <номер_правила> destination address-group <имя_группы>.

16.2.16 filter <имя> rule <номер_правила> destination port <порт>

Указание номера сетевого порта получателя для проверки соответствия в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> destination port <порт>
delete filter <имя> rule <номер_правила> destination port <порт>
show filter <имя> rule <номер_правила> destination port
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
    rule номер_правила {
        destination {
            port порт
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

порт

Порт назначения, используемый для проверки соответствия. Допустимые значения приведены в таблице ниже.

Таблица 68 – Формат указания порта получателя

Значение	**Описание**
<text>	Имя порта (любое из файла /etc/services)
<0-65535>	Номер порта
<start>-<end>	Диапазон портов

Возможно также задание списка через запятую, например: "22,telnet,http,123,1001-1005".

Возможно также задание инвертированного списка с помощью "!", например: "!22,telnet,http,123,1001-1005".

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать номера сетевого порта получателя в правиле фильтрации трафика IPv4. Может быть указан только для протоколов TCP, UDP, SCTP и DCCP. Предварительно должен быть определен протокол при помощи команды *filter <имя> rule <номер_правила> protocol <протокол>*.

В том случае если явно указаны адрес и номер порта, для пакета устанавливается соответствие критериям правила в том и только том случае, если совпадает как адрес, так и номер порта.

ПРИМЕЧАНИЕ Для указания порта получателя порт задается либо данной командой, либо указанием группы портов командой filter <имя> rule <номер_правила> destination port-group <имя_группы>. Параллельное использование обоих механизмов не допускается.

Форма **set** данной команды позволяет указать или изменить номер сетевого порта получателя.

Форма **delete** данной команды позволяет удалить настройку номера сетевого порта получателя.

Форма **show** данной команды позволяет отобразить настройку номера сетевого порта получателя.

16.2.17 filter <имя> rule <номер_правила> destination port-group <имя_группы>

Указание группы портов для проверки соответствия порта получателя сетевого пакета в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> destination port-group <имя_группы>
delete filter <имя> rule <номер_правила> destination port-group <имя_группы>
show filter <имя> rule <номер_правила> destination port-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
    rule номер_правила {
        destination {
            port-group имя_группы
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

имя_группы

Имя группы портов.

Таблица 69 - Допустимые значения для группы доменов

Значение	Описание
<text>	Имя группы
!<text>	Все группы кроме указанной

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет использовать заранее определенную группу портов для сопоставления с номером порта получателя пакета. Группа должна быть предварительно определена при помощи команды *groups port-group <имя_группы>*. Может быть указана только одна группа.

Соответствие для пакета устанавливается в том случае, если номер порта назначения (получателя) пакета совпадает с одним из портов, входящих в состав указанной группы.

ПРИМЕЧАНИЕ Для указания порта получателя порт задается либо указанием группы портов данной командой, либо указанием портов командой filter <имя> rule <номер_правила> destination port <порт>. Параллельное использование обоих механизмов не допускается.

Форма **set** данной команды используется для указания группы портов получателя для проверки соответствия.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.18 filter <имя> rule <номер_правила> disable

Отключение указанного правила фильтрации трафика IPv4.

Синтаксис

```
set filter <имя>  rule <номер_правила> disable
delete filter <имя>  rule <номер_правила> disable
show filter <имя>  rule <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      disable
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

Значение по умолчанию

Правило включено (используется).

Указания по использованию

Данная команда позволяет отключить правило фильтрации трафика IPv4. Это может быть полезно при проверке того, как фильтр трафика функционирует без указанного правила. При этом не нужно удалять и заново создавать данное правило.

Форма **set** данной команды используется для отключения правила фильтрации трафика.

Форма **delete** данной команды используется для включения правила фильтрации трафика.

Форма **show** данной команды используется для отображения настройки правила фильтрации трафика.

16.2.19 filter <имя> rule <номер_правила> dscp <значение>

Установка соответствия на основе поля DSCP.

Синтаксис

```
set filter <имя> rule <номер_правила> dscp <значение>
delete filter <имя> rule <номер_правила> dscp <значение>
show filter <имя> rule <номер_правила> dscp
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      dscp значение
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

значение

Значение поля DSCP, на основе которого устанавливается соответствие. Допустимые значения приведены в таблице ниже.

Таблица 70 - Допустимые значения поля DSCP

Значение	Описание
<x>	Численное значение DSCP (где *x* - десятичное значение в диапазоне от *0* до *63*)
<x>	Численное значение DSCP (где *x* - шестнадцатеричное значения в диапазоне от *0* до *3F* в формате *0xYZ*, например, *0x2E* или *0x2e*)
default	Значение DSCP по умолчанию, соответствующее стандартной пересылке (шестнадцатеричное значение - *0x0*, двоичное значение - *000000*)
EF	Значение Express Forwarding, соответствующее экстренной пересылке
AFxy	Значение Assured Forwarding, соответствующее гарантированной пересылке (*x* находится в диапазоне от *1* до *4*, y - от *1* до *3*)
CSx	Значение Class Selector поддерживает обратную совместимость с полем приоритета IP (*x* находится в диапазоне от *1* до *7*)

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать проверку соответствия на основе поля DSCP.

Форма **set** данной команды позволяет указать проверку соответствия на основе поля DSCP.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.20 filter <имя> rule <номер_правила> ecn ip ect <значение>

Установка соответствия на основе флага ECT в заголовке IP.

Синтаксис

```
set filter <имя> rule <номер_правила> ecn ip ect <значение>
delete filter <имя> rule <номер_правила> ecn ip ect <значение>
show filter <имя> rule <номер_правила> ecn ip ect
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      ecn {
         ip {
            ect значение
        }
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

значение

Значение флага ECT в заголовке IP, на основе которого устанавливается соответствие. Допустимые значения приведены в таблице ниже.

Таблица 71 - Допустимые значения флага ECT

Значение	Описание
<x>	Значение флага ECN (где *x* - целое в диапазоне от *0* до *3*)
!<x>	Все значения флага ECN, кроме указанного (где *x* - целое в диапазоне от *0* до *3*)

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать проверку соответствия на основе значения флага ECT в заголовке IP.

Форма **set** данной команды позволяет указать проверку соответствия на основе значения флага ECT в заголовке IP.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.21 filter <имя> rule <номер_правила> ecn tcp cwr <значение>

Установка соответствия на основе флага CWR в заголовке TCP.

Синтаксис

```
set filter <имя> rule <номер_правила> ecn tcp cwr <значение>
delete filter <имя> rule <номер_правила> ecn tcp cwr <значение>
show filter <имя> rule <номер_правила> ecn tcp cwr
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      ecn {
         tcp {
           cwr значение
         }
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

значение

Значение флага CWR в заголовке TCP, на основе которого устанавливается соответствие. Допустимые значения: 0, 1.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать проверку соответствия на основе значения флага CWR в заголовке TCP. Предварительно должен быть определен протокол TCP для правила фильтрации при помощи команды *filter <имя> rule <номер_правила> protocol tcp*.

Форма **set** данной команды позволяет указать проверку соответствия на основе значения флага CWR в заголовке TCP.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.22 filter <имя> rule <номер_правила> ecn tcp ece <значение>

Установка соответствия на основе флага ECE в заголовке TCP.

Синтаксис

```
set filter <имя>  rule <номер_правила> ecn tcp ece <значение>
delete filter <имя>  rule <номер_правила> ecn tcp ece <значение>
show filter <имя>  rule <номер_правила> ecn tcp ece
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      ecn {
         tcp {
            ece значение
         }
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

значение

Значение флага ECE в заголовке TCP, на основе которого устанавливается соответствие. Допустимые значения: 0, 1.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать проверку соответствия на основе значения флага ECE в заголовке TCP. Предварительно должен быть определен протокол TCP для правила фильтрации при помощи команды *filter <имя> rule <номер_правила> protocol tcp*.

Форма **set** данной команды позволяет указать проверку соответствия на основе значения флага ECE в заголовке TCP.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.23 filter <имя> rule <номер_правила> exclude

Исключение правила из фильтра.

Синтаксис

```
set filter <имя> rule <номер_правила> exclude
delete filter <имя> rule <номер_правила> exclude
show filter <имя> rule <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
     exclude
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

exclude

При указании данного параметра будут исключены пакеты, удовлетворяющие критериям правила фильтрации трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет исключать пакеты, удовлетворяющие критериям правила.

Форма **set** данной команды позволяет указать правило, которое необходимо исключить из набора правил фильтра.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

ПРИМЕЧАНИЕ При применении исключения правила трафик, удовлетворяющий критериям такого правила, будет считаться не соответствующим заданному фильтру. Проверка соответствия дальнейшим правилам этого фильтра проводиться не будет.

ПРИМЕЧАНИЕ Следует учитывать, что правило исключения не отменяет соответствие трафика предыдущим правилам фильтра. То есть если трафик удовлетворяет критериям хотя бы одного предыдущего правила, то он считается соответствующим заданному фильтру несмотря на соответствие критериям правила исключения.

16.2.24 filter <имя> rule <номер_правила> fragment <тип>

Указание типа проверки соответствия для фрагментированных пакетов.

Синтаксис

```
set filter <имя> rule <номер_правила> fragment <тип>
delete filter <имя> rule <номер_правила> fragment <тип>
show filter <имя> rule <номер_правила> fragment
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
```

```
        fragment {
            тип
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

тип

Тип проверки соответствия для фрагментированных пакетов. Допустимые значения:

match-frag: Соответствие устанавливается для второго и последующих фрагментов фрагментированного пакета;

match-non-frag: Соответствие устанавливается для первого фрагмента фрагментированного пакета, а также для нефрагментированного пакета.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать тип проверки соответствия для фрагментированных пакетов.

ПРИМЕЧАНИЕ Обнаружение фрагментированных пакетов не работает для правил межсетевого экранирования локального трафика.

ПРИМЕЧАНИЕ При наличии в конфигурации фильтра по состояниям соединений state или трансляции адресов NAT на устройстве производится дефрагментация пакетов. В таком случае обнаружение фрагментированных пакетов данным фильтром не будет отрабатывать.

Форма **set** данной команд позволяет указать тип проверки соответствия для фрагментированных пакетов.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.25 filter <имя> rule <номер_правила> icmp type <тип>

Указание кода и типа ICMP для правила фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> icmp type <тип>
delete filter <имя> rule <номер_правила> icmp type
show filter <имя> rule <номер_правила> icmp type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
    rule номер_правила {
```

```
        icmp {
            type тип
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

тип

Корректный тип ICMP. Допустимые значения приведены в таблице ниже.

Таблица 72 - Допустимые значения проверки соответствия типов icmp

Значение	Описание
<0-255>	Проверка соответствия по номеру типа сообщения
<0-255>/<0-255>	Проверка соответствия по номеру типа сообщения и код сообщения
<текст>	Проверка соответствия по типу сообщения в текстовом формате (например: network-unreachable)
!<0-255>	Соответствие будет установлено для всех типов сообщений, кроме указанного номера типа сообщения
!<0-255>/<0-255>	Соответствие будет установлено для всех типов сообщений, кроме указанного номера типа и кода сообщения
!<текст>	Соответствие будет установлено для всех типов сообщений, кроме указанного

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет определить типы ICMP сообщений, к которым применяется данное правило, например, эхо-запрос или эхо-ответ. Для пакетов ICMP указанного типа будет установлено соответствие данному правилу. Предварительно должен быть определен протокол ICMP при помощи команды *filter <имя> rule <номер_правила> protocol icmp*.

Форма **set** данной команды используется для указания кода и типа ICMP для указанного правила

Форма **delete** данной команды используется для удаления кода или типа ICMP для указанного правила.

Форма **show** данной команды используется для отображения кода или типа ICMP для указанного правила.

16.2.26 filter <имя> rule <номер_правила> ipsec <тип>

Установка соответствия для пакетов, получаемых внутри IPSec соединения.

Синтаксис

```
set filter <имя> rule <номер_правила> ipsec <тип>
delete filter <имя> rule <номер_правила> ipsec <тип>
show filter <имя> rule <номер_правила> ipsec
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
    rule номер_правила {
```

```
        ipsec {
            тип
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

тип

Тип проверки соответствия для входящих пакетов IPSec. Допустимые значения:

match-ipsec: Установка соответствия для пакетов, получаемых внутри IPSec соединения;

match-none: Установка соответствия для пакетов, не использующих IPSec соединение.

Значение по умолчанию

Отсутствует.

Указания по использованию

При установленном значении **match-ipsec** и указании дополнительных параметров внутри одного правила фильтрации, позволяет фильтровать трафик, получаемый внутри IPSec соединения. Значение **match-none** соответствует "обычному" трафику, не использующему IPSec в качестве сетевого протокола.

Форма **set** данной команды используется для указания типа пакетов, для которых будет установлено соответствие для указанного правила.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.27 filter <имя> rule <номер_правила> ipv4options mode <режим>

Установка режима для критерия соответствия на основе поля опций в заголовке IPv4-пакета.

Синтаксис

```
set filter <имя> rule <номер_правила> ipv4options mode <режим>
delete filter <имя> rule <номер_правила> ipv4options mode <режим>
show filter <имя> rule <номер_правила> ipv4options mode
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
    rule номер_правила {
        ipv4options {
            mode режим
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

режим

Режим, на основании которого устанавливается критерий соответствия пакетов на основе опций IP. Допустимые значения:

and: Требуется соответствие всем опциям в заголовке IP-пакета;

or: Требуется соответствие хотя бы одной опции в заголовке IP-пакета.

Значение по умолчанию

По умолчанию установлено значение **and**.

Указания по использованию

Данная команда используется для установки режима для критерия соответствия на основе поля опций в заголовке IPv4-пакета. Опции задаются с помощью команды filter <имя> rule <номер_правила> ipv4options opts <список_опций>.

Форма **set** данной команды используется для указания режима для критерия соответствия на основе поля опций в заголовке IPv4-пакета.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.28 filter <имя> rule <номер_правила> ipv4options opts <список_опций>

Указание списка опций IP, которые будут использоваться в критерии соответствия на основе поля опций в заголовке IP-пакета.

Синтаксис

```
set filter <имя> rule <номер_правила> ipv4options opts <список_опций>
delete filter <имя> rule <номер_правила> ipv4options opts <список_опций>
show filter <имя> rule <номер_правила>  ipv4options opts
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      ipv4options {
         opts список_опций
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

список_опций

Список опций IP, на основе которых будет устанавливаться соответствие для пакетов. Допустимые значения приведены в таблице ниже.

Таблица 73 - Допустимые значения опций в заголовке IP-пакета

Значение	**Описание**
1	nop: опция No Operation **[см. RFC1108]**
2	security: опция Security **[см. RFC1108]**
3	lsrr: опция Loose Source Route **[см. RFC791]**
4	timestamp: опция Time Stamp **[см. RFC781, RFC791]**
7	record-route: опция Record Route **[см. RFC791]**
9	ssrr: опция Strict Source Route **[см. RFC791]**
11	mtu-probe: опция MTU Probe**[см. RFC1063]**
12	mtu-reply: опция MTU Reply **[см. RFC1063]**
18	traceroute: опция Traceroute **[см. RFC1393]**
20	router-alert: опция Router Alert **[см. RFC2113]**

Допускается перечисление опций через запятую. При указании "**!**" перед названием опции, соответствие будет найдено, если эта опция не установлена в заголовке пакета.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для установки списка опций IP, которые будут использоваться в критерии соответствия на основе поля опций в заголовке IPv4-пакета.

В критерии соответствия опции могут быть использованы в режиме логического И, либо логического ИЛИ. Режим задается с помощью команды *filter <имя> rule <номер_правила> ipv4options mode <режим>*.

Форма **set** данной команды используется для указания списка опций для критерия соответствия на основе поля опций в заголовке IPv4-пакета.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.29 filter <имя> rule <номер_правила> l7protocol <протокол>

Указание протокола для фильтрации пакетов на прикладном уровне.

Синтаксис

```
set filter <имя> rule <номер_правила> l7protocol <протокол>
delete filter <имя> rule <номер_правила> l7protocol <протокол>
show filter <имя> rule <номер_правила> l7protocol
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      l7protocol протокол
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

протокол

Имя протокола прикладного уровня, используемого для фильтрации пакетов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для включения фильтрации сетевых пакетов на прикладном уровне. Для фильтрации на прикладном уровне используется механизм регулярных выражений, который позволяет определить тип используемого протокола.

При использовании фильтрации на прикладном уровне необходимо учитывать, что для корректной работы механизма классификатор трафика должен видеть весь имеющий значение для классификации трафик. Для этого под правило фильтрации трафика, в котором применяется фильтрация на прикладном уровне, должны подпадать все разновидности трафика, генерируемые классифицируемым протоколом. Так, например, если в таком правиле будет учитываться только трафик, идущий в одном направлении, но не будет учитываться трафик, идущий в рамках тех же соединений в обратную сторону, фильтрация в ряде случаев может выполняться некорректно.

Так как механизм фильтрации на прикладном уровне требует больших системных ресурсов по сравнению с фильтрацией на основе параметров источника и отправителя, рекомендуется в тех случаях, когда это возможно использовать механизм фильтрации на основе таких параметров получателя и отправителя, как номер используемого сетевого порта или IP-адрес.

Фильтрация на прикладном уровне может быть использована в тех случаях, когда:

- требуется установить соответствие для пакетов протоколов, использующих номера портов, которые не могут быть заранее предсказаны;
- требуется установить соответствие для пакетов протоколов при использовании нестандартных номеров портов (например, HTTP на порту 1111);
- требуется распознать протоколы, использующие одинаковые номера портов (например, обмен файлами P2P, использующий порт 80).

Фильтрация на прикладном уровне может быть использована для контроля полосы пропускания для указанных протоколов, для учета пакетов указанных протоколов или для блокировки пакетов. При использовании фильтрации на прикладном уровне для блокировки пакетов указанных протоколов без дополнительных мер следует помнить, что могут возникать как ошибочные срабатывания (один протокол похож на другой), так и ошибочные несрабатывания фильтров (приложения могут маскировать свой протокол обмена способами, не учитываемыми в фильтре).

Форма **set** данной команды позволяет указать протокол для фильтрации на прикладном уровне.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.30 filter <имя> rule <номер_правила> length

Указание параметров, ограничивающих длину пакетов для правила фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> length [layer <уровень> | value <длина>]
delete filter <имя> rule <номер_правила> length [layer | value]
show filter <имя> rule <номер_правила> length [layer | value]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
     length {
         layer уровень
         value длина
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

уровень

Уровень сетевой модели TCP/IP. Указать уровень согласно сетевой модели TCP/IP, на котором будет производиться проверка длины пакета. Допустимые значения приведены в таблице ниже.

Таблица 74 - Допустимые значения уровней сетевой модели TCP/IP

Значение	**Описание**
layer3	Сетевой уровень
layer4	Транспортный уровень
layer5	Прикладной уровень

длина

Длина пакета. Допустимые значения приведены в таблице ниже.

Таблица 75 - Допустимые значения длины пакета

Значение	**Описание**
<0-4294967295>	Соответствие для пакетов указанной длины
!<0-4294967295>	Соответствие для всех пакетов, за исключением имеющих указанную длину
<x-y>	Соответствие для пакетов указанного диапазона длин
!<x-y>	Соответствие для всех пакетов, кроме имеющих указанный диапазон длин

Значение по умолчанию

Ограничения не установлены.

Указания по использованию

Данная команда позволяет указать параметры, ограничивающие длину пакетов в правиле фильтрации трафика IPv4.

Форма **set** данной команды используется для указания параметров, ограничивающих длину пакетов в правиле фильтрации трафика.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.31 filter <имя> rule <номер_правила> limit connection-rate

Указание параметров, ограничивающих частоту прохождения пакетов для соединения в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> limit connection-rate [above <макс_частота> | burst <размер> | destination-mask <маска_получателя> | group-by <режим> | source-mask <маска_источника> | upto <мин_частота>]

delete filter <имя> rule <номер_правила> limit connection-rate [above | burst | destination-mask | group-by | source-mask | upto]

show filter <имя> rule <номер_правила> limit connection-rate [above | burst | destination-mask | group-by | source-mask | upto]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
    rule номер_правила {
        limit {
            connection-rate {
                above макс_частота
                burst размер
                destination-mask маска_получателя
                group-by режим
                source-mask маска_источника
                upto мин_частота
            }
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

макс_частота

Максимальная частота прохождения сетевых пакетов, для которых было установлено соответствие критериям правила. Время может быть указано в следующих единицах: **second** (секунды), **minute** (минуты), **hour** (часы), а также **day** (дни). Допустимые значения для частоты прохождения сетевых пакетов приведены в таблице ниже.

Таблица 76 - Допустимые значения частоты прохождения сетевых пакетов

Значение	Описание
<1-10000>	Число пакетов в секунду
<1-10000>/second	Число пакетов в секунду
<1-600000>/minute	Число пакетов в минуту
<1-36000000>/hour	Число пакетов в час
<1-864000000>/day	Число пакетов за день

размер

Размер буфера групп пакетов. Задает число пакетов, которые могут быть переданы со скоростью, превышающей указанную. По умолчанию установлено значение равное 1, которое не допускает передачи

групп пакетов со скоростью превышающей установленную. Значение должно находиться в диапазоне от 1 до 10000.

маска_получателя

Маска для группировки соединений по IP-адресу получателя. Значение должно находиться в диапазоне от 0 до 32.

режим

Режим группировки соединений. Допустимые значения для режима группировки соединений приведены в таблице ниже.

Таблица 77 - Допустимые значения режима группировки соединений

Значение	**Описание**
destination-address	Группировка по IPv4-адресу получателя
destination-port	Группировка по порту получателя
source-address	Группировка по IPv4-адресу отправителя
source-port	Группировка по порту отправителя

маска_источника

Маска для группировки соединений по IP-адресу отправителя. Значение должно находиться в диапазоне от 0 до 32.

мин_частота

Минимальная частота прохождения сетевых пакетов, для которых было установлено соответствие критериям правила. Ограничения на значения аналогичны значениям максимальной частоты.

Значение по умолчанию

Ограничение не установлено.

Указания по использованию

Данная команда позволяет указать параметры, ограничивающие частоту прохождения сетевых пакетов для соединения в правиле фильтрации трафика IPv4. При создании правила фильтрации, ограничивающего частоту прохождения сетевых пакетов для соединения, указание режима группировки соединений, а также максимальной или минимальной частоты является обязательным. Может быть указано либо максимальная, либо минимальная частота.

Форма **set** данной команды используется для указания параметров, ограничивающих частоту прохождения пакетов для соединения.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.32 filter <имя> rule <номер_правила> limit connections

Указание параметров, ограничивающих количество соединений в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила>  limit connections [above <мин_кол-во> | group-by <режим>| mask <маска> | upto <макс_кол-во>]

delete filter <имя> rule <номер_правила> limit connections [above | mask]

show filter <имя> rule <номер_правила> limit connections [above | mask]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
    rule номер_правила {
        limit {
```

```
            connections {
               above мин_кол-во
               group-by режим
               mask маска
               upto макс_кол-во
            }
         }
      }
   }
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

мин_кол-во

Минимальное количество соединений. Значение должно находиться в диапазоне от 0 до 4294967295.

режим

Режим группировки соединений. Допустимые значения:

destination: Группировка по IPv4-адресу получателя;

source: Группировка по IPv4-адресу отправителя.

маска

Маска для группировки соединений по IP-адресу. Значение должно находиться в диапазоне от 0 до 32.

макс_кол-во

Максимальное количество соединений. Значение должно находиться в диапазоне от 0 до 4294967295.

Значение по умолчанию

Ограничение не установлено.

Указания по использованию

Данная команда позволяет указать параметры, ограничивающие количество соединений в правиле фильтрации трафика IPv4. При создании правила фильтрации, ограничивающего количество соединений, указание минимального или максимального числа соединений является обязательным. Может быть указано либо максимальное, либо минимальное количество соединений.

Форма **set** данной команды используется для указания параметров, ограничивающих количество соединений в правиле фильтрации трафика.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.33 filter <имя> rule <номер_правила> limit packet-rate

Указание параметров, ограничивающих частоту прохождения пакетов в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила>  limit packet-rate [burst <размер> | rate <частота>]
delete filter <имя> rule <номер_правила> limit packet-rate [burst | rate]
show filter <имя> rule <номер_правила> limit packet-rate [burst | rate]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      limit {
         packet-rate {
            burst размер
            rate частота
         }
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

размер

Размер буфера групп пакетов. Максимальное число пакетов, которые могут быть переданы со скоростью, превышающей указанную. По умолчанию установлено значение равное 1, которое не допускает передачи групп пакетов со скоростью превышающей установленную. Значение должно находиться в диапазоне от 1 до 10000.

частота

Частота прохождения сетевых пакетов, для которых было установлено соответствие критериям правила. Время может быть указано в следующих единицах: **second** (секунды), **minute** (минуты), **hour** (часы), а также **day** (дни). Допустимые значения для частоты прохождения сетевых пакетов приведены в таблице ниже.

Таблица 78 - Допустимые значения частоты прохождения сетевых пакетов

Значение	Описание
<1-10000>	Число пакетов в секунду
<1-10000>/second	Число пакетов в секунду
<1-600000>/minute	Число пакетов в минуту
<1-36000000>/hour	Число пакетов в час
<1-864000000>/day	Число пакетов за день

Значение по умолчанию

Ограничение не установлено.

Указания по использованию

Данная команда используется для ограничения частоты прохождения сетевых пакетов, для которых установлено соответствие данному правилу. Для ограничения частоты прохождения входящих сетевых пакетов используется фильтр TBF (Token Bucket Filter), который позволяет административно задать требуемую пропускную способность, а также возможность ее превышения для коротких групп пакетов.

Для реализации TBF используется буфер (bucket), который постоянно заполняется маркерами (token) с установленной скоростью (token rate). Наиболее важным параметром буфера является его размер, то есть число маркеров, которое в нем может содержаться. Каждый прибывающий маркер сопоставляется с одним пакетом данных из очереди данных, после чего удаляется из буфера. При работе данного алгоритма возможны три различных варианта:

Данные прибывают со скоростью **равной** скорости входящих маркеров. В этом случае каждый пакет имеет соответствующий маркер и проходит очередь без задержки.

Данные прибывают со скоростью **меньшей** скорости поступления маркеров. В этом случае лишь часть существующих маркеров будет уничтожаться, таким образом, они станут накапливаться до размера буфера. Накопленные маркеры могут использоваться для передачи групп пакетов со скоростью, превышающей установленную скорость прибывающих маркеров.

Данные прибывают **быстрее**, чем маркеры. Это означает, что в определенный момент в буфере не останется маркеров, что заставит алгоритм приостановить передачу данных. Эта ситуация называется "превышением". Если пакеты продолжают поступать, они начинают уничтожаться.

Форма **set** данной команды используется для указания параметров, ограничивающих частоту прохождения пакетов.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.34 filter <имя> rule <номер_правила> log <состояние>

Включение или отключение регистрации для действий правила фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> log <состояние>
delete filter <имя> rule <номер_правила> log <состояние>
show filter <имя> rule <номер_правила> log
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      log состояние
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

состояние

Включение или отключение регистрации действий фильтра трафика. Допустимые значения:

enable: Включить регистрацию действий;

disable: Отключить регистрацию действий.

Значение по умолчанию

Регистрация действий отключена.

Указания по использованию

Данная команда используется для включения или отключения регистрации действия для указанного правила.

ПРИМЕЧАНИЕ Регистрация действия происходит только используемого фильтра, т.е такого фильтра,

который применен к какой-либо политике. Эта политика, в свою очередь, должна быть применена к какому-либо направлению трафика. В противном случае фильтр считается настроенным, но не активным.

Сообщения регистрации для правил фильтрации трафика записываются в журнал регистрации от имени программы **kernel** с уровнем серьезности **warning**. При регистрации пакета в журнале регистрации указывается имя фильтра и его номер.

Например, для сетевого пакета который попадает под правило 10 фильтра трафика с именем **test**, в журнал регистрации будет помещена запись **[test-10]**. Если правило фильтра трафика было правилом исключения (атрибут **exclude**), то в журнал регистрации будет помещена запись **[test-10-E]**.

Форма **set** данной команды позволяет включить регистрацию указанного правила.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.35 filter <имя> rule <номер_правила> p2p <имя_приложения>

Указание одноранговогo приложения для фильтрации его IPv4-пакетов на прикладном уровне.

Синтаксис

```
set filter <имя> rule <номер_правила> p2p <имя_приложения>
delete filter <имя> rule <номер_правила> p2p <имя_приложения>
show filter <имя> rule <номер_правила> p2p
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
     p2p {
         имя_приложения
      }
  }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

имя_приложения

Обязательный. Соответствие устанавливается для пакетов одноранговогo приложения. Допустимые значения приведены в таблице ниже.

Таблица 79 - Допустимые значения одноранговых приложений

Значение	Описание
all	Соответствие устанавливается для пакетов любого из приложений, перечисленных в данной таблице
applejuice	Соответствие устанавливается для пакетов приложения AppleJuice
bittorrent	Соответствие устанавливается для пакетов приложения BitTorrent
directconnect	Соответствие устанавливается для пакетов приложения Direct Connect
edonkey	Соответствие устанавливается для пакетов приложения eDonkey/eMule

gnutella	Соответствие устанавливается для пакетов приложения Gnutella
kazaa	Соответствие устанавливается для пакетов приложения KaZaA

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания однорангового приложения, пакеты которого будут фильтроваться. Фильтрация происходит на прикладном уровне. Для пакетов, отправленных указанным приложением или предназначенных для него, будет установлено соответствие критериям данного правила. В правиле может быть указано несколько одноранговых приложений.

Форма **set** данной команды используется для указания однорангового приложения, к пакетам которого будет применяться правило.

Форма **delete** данной команды используется для удаления настройки однорангового приложения для указанного правила.

Форма **show** данной команды используется для отображения настройки.

16.2.36 filter <имя> rule <номер_правила> probability <вероятность>

Указание вероятности срабатывания правила в процентах.

Синтаксис

```
set filter <имя> rule <номер_правила> probability <вероятность>
delete filter <имя> rule <номер_правила> probability
show filter <имя> rule <номер_правила> probability
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      probability вероятность
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

вероятность

Вероятность срабатывания правила в процентах. Обязательный параметр. Значение должно находиться в диапазоне от 1 до 99.

Значение по умолчанию

Не установлено.

Указания по использованию

Данная команда используется для указания вероятности срабатывания правила в процентах от 1 до 99.

Форма **set** данной команды используется для указания вероятности срабатывания правила.

Форма **delete** данной команды используется для удаления установленного значения.

Форма **show** данной команды используется для отображения установленного значения для вероятности срабатывания правила.

16.2.37 filter <имя> rule <номер_правила> protocol <протокол>

Указание протокола для фильтрации пакетов.

Синтаксис

```
set filter <имя> rule <номер_правила> protocol <протокол>
delete filter <имя> rule <номер_правила> protocol <протокол>
show filter <имя> rule <номер_правила> protocol
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      protocol протокол
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

протокол

Обязательный. Могут быть использованы любые наименования протоколов или их номера, определенные в файле **/etc/protocols**. Допустимые значения приведены в таблице ниже.

Таблица 80 - Допустимые значения для указания протокола

Значение	Описание
All	Соответствие устанавливается для всех протоколов IPv4
tcp_udp	Соответствие устанавливается для протоколов TCP и UDP
<0-255>	Соответствие устанавливается для указанного номера протокола IPv4
<text>	Соответствие устанавливается для указанного имени протокола IPv4
!<0-255>	Соответствие устанавливается для всех протоколов IPv4, кроме указанного
!<text>	Соответствие устанавливается для всех протоколов IPv4, кроме указанного

Значение по умолчанию

По умолчанию определены все протоколы.

Указания по использованию

Данная команда используется для определения критерия соответствия на основе указанного протокола. Для пакетов указанного протокола будет установлено соответствие данному правилу.

Следует с осторожностью включать в набор правил более одного правила, определяющего исключения (правило, в котором указывается восклицательный знак "!"). Правила фильтра трафика выполняются по порядку, при этом последовательность правил, определяющих исключения, может привести к непредсказуемым результатам.

Форма **set** данной команды используется для указания протокола, к пакетам которого будет применяться указанное правило.

Форма **delete** данной команды используется для удаления установленного значения.

Форма **show** данной команды используется для отображения установленного значения.

16.2.38 filter <имя> rule <номер_правила> quota overall

Настройка квотирования фильтрации пакетов по всему объёму данных или числу пакетов.

Синтаксис

```
set filter <имя> rule <номер_правила> quota overall [invert | mode <режим_квотирования> | upto <макс_число>]
delete filter <имя> rule <номер_правила> quota overall [invert | mode | upto]
show filter <имя> rule <номер_правила> quota overall [invert | mode | upto]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      quota {
         overall {
            invert
            mode режим_квотирования
            upto макс_число
         }
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

Invert

Необязательное ключевое слово. Если оно не указано, то правило будет срабатывать до тех пор, пока заданное значение счётчика не будет превышено. Если ключевое слово **invert** указано, то поведение будет обратным: правило не будет срабатывать, пока заданное значение не будет превышено.

режим_квотирования

Определяет один из двух режимов квотирования:

bytes: Квотирование по объёму данных;

packets: Квотирование по числу пакетов.

макс_число

Определяет максимальный объём данных или число пакетов. Объём данных может быть указан в следующих единицах: kb (килобайты), mb (мегабайты), gb (гигабайты). Допустимые значения приведены в таблице ниже.

Таблица 81 - Допустимые значения для указания максимального объёма данных или числа пакетов

Значение	Описание
<1-18446744073709551615>	Максимальное количество пакетов, если указан режим packets (2^64 -1)
<1-18446744073709551615>	Максимальный объём данных (в байтах), если указан режим bytes (2^64 -1)

<1-18014398509481983>kb	Максимальный объём данных (в килобайтах), только для режима bytes (2^54 -1)
<1-17592186044415>mb	Максимальный объём данных (в мегабайтах), только для режима bytes (2^44 -1)
<1-17179869183>gb	Максимальный объём данных (в гигабайтах), только для режима bytes (2^34 -1)

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать режим квотирования и объём квоты пакетов для правила фильтрации трафика IPv4 без учёта направления движения пакетов.

Форма **set** данной команды используется для указания режима квотирования и объёма квоты пакетов для правила фильтрации трафика.

Форма **delete** данной команды используется для удаления установленного значения.

Форма **show** данной команды используется для отображения установленного значения.

16.2.39 filter <имя> rule <номер_правила> quota per-connection

Настройка квотирования фильтрации пакетов по объёму данных или числу пакетов на соединение.

Синтаксис

```
set filter <имя> rule <номер_правила>  quota per-connection [count-direction <направление_движения> | mode <режим_квотирования>| upto <макс_число>]
```

```
delete filter <имя> rule <номер_правила> quota per-connection [count-direction | mode | upto]
```

```
show filter <имя> rule <номер_правила>  quota per-connection [count-direction | mode | upto]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
    rule номер_правила {
        quota {
            per-connection {
                count-direction направление_движения
                mode режим_квотирования
                upto макс_число
            }
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

направление_движения

Необязательный. Направление движения пакетов, которое стоит учитывать. Допустимые значения для направления движения пакетов приведены в таблице ниже.

Таблица 82 - Допустимые значения для направления движения пакетов

Значение	Описание
original	Учитываются пакеты от инициатора соединения
reply	Учитываются пакеты к инициатору соединения
both	Учитываются пакеты для обоих направлений

По умолчанию учитываются пакеты для обоих направлений.

режим_квотирования

Определяет один из двух режимов квотирования:

bytes: Квотирование по объёму данных;

packets: Квотирование по числу пакетов.

макс_число

Определяет максимальный объём данных или число пакетов. Объём данных может быть указан в следующих единицах: kb (килобайты), mb (мегабайты), gb (гигабайты). Допустимые значения приведены в таблице ниже.

Таблица 83 - Допустимые значения для указания максимального объёма данных или числа пакетов

Значение	Описание
<1-4294967295>	Максимальное количество пакетов, если указан режим packets (2^32 -1)
<1-4294967295>	Максимальный объём данных (в байтах), если указан режим bytes (2^32 -1)
<1-4194303>kb	Максимальный объём данных (в килобайтах), только для режима bytes (2^22 -1)
<1-4095>mb	Максимальный объём данных (в мегабайтах), только для режима bytes (2^12 -1)
<1-3>gb	Максимальный объём данных (в гигабайтах), только для режима bytes (2^2 -1)

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать режим квотирования и объём квоты пакетов для правила фильтрации трафика IPv4 с учётом направления движения пакетов.

Форма **set** данной команды используется для указания режима квотирования и объёма квоты пакетов для правила фильтрации трафика.

Форма **delete** данной команды используется для удаления установленного значения.

Форма **show** данной команды используется для отображения установленного значения.

16.2.40 filter <имя> rule <номер_правила> recent

Установка соответствия для сетевых пакетов от недавно встречавшихся отправителей.

Синтаксис

```
set filter <имя> rule <номер_правила> recent [count <счетчик> | time <секунды>]
delete filter <имя> rule <номер_правила> recent [count | time]
show filter <имя> rule <номер_правила> recent [count | time]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      recent {
         count счетчик
```

```
            time секунды
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

счетчик

Обязательный. Количество пакетов с одинаковым IP-адресом отправителя, необходимое для срабатывания правила. Значение должно находиться в диапазоне от 1 до 20.

секунды

Обязательный. Количество времени, указываемое в секундах, в течение которого будет происходить подсчет пакетов от одного отправителя. Значение должно находиться в диапазоне от 1 до 4294967295.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет установить соответствие для сетевых пакетов, пришедших от недавно встречавшихся отправителей.

Форма **set** данной команды позволяет установить настройку для проверки соответствия на основе адресов недавно встречавшихся отправителей.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.41 filter <имя> rule <номер_правила> sctp chunk-type

Установка параметров протокола SCTP для проверки соответствия в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя>  rule <номер_правила> sctp chunk-type [invert | logic <режим_сопоставления> | type <тип>]

delete filter <имя>  rule <номер_правила> sctp chunk-type [invert | logic | type <тип>]

show filter <имя>  rule <номер_правила> sctp chunk-type [logic | type]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила
{      sctp {
         chunk-type {
            invert
            logic режим_сопоставления
            type {
               тип
```

```
                    }
                }
            }
        }
    }
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

invert

Необязательное ключевое слово. Если оно указано, то производится инверсия сопоставления.

режим_сопоставления

Обязательный. Логика обработки пакетов с указанными типами блоков. Допустимые значения приведены в таблице ниже.

Таблица 84 - Допустимые значения для режима сопоставления пакетов с указанными типами блоков

Значение	**Описание**
any	Соответствие устанавливается при совпадении любого из указанных типов
all	Соответствие устанавливается при совпадении всех указанных типов
only	Соответствие устанавливается при совпадении всех указанных типов и отсутствию иных типов

По умолчанию используется режим сопоставления **any**.

тип

Обязательный. Тип блока для сопоставления. Допустимые значения типов блоков приведены в таблице ниже.

Таблица 85 - Допустимые значения для указания типов блоков

Значение	**Описание**
abort	Разрыв ассоциации (ABORT, код 6)
asconf	Смена адресной настройки (ASCONF, код 193)
asconf-ack	Подтверждение адресной конфигурации (ASCONF ACK, код 128)
cookie-ack	Подтверждение маркера (COOKIE ACK, код 11)
cookie-echo	Маркерное отражение (COOKIE ECHO, код 10)
data	Данные (DATA, код 0)
ecn-cwr	Окно перегрузки уменьшено (CWR, код 13)
ecn-ecne	Отражение явного уведомления о перегруженности (ECN ECHO, код 12)
error	Ошибка взаимодействия (ERROR, код 9)
forward-tsn	Смещение накопленного порядкового номера передачи (FORWARD TSN, код 192)
heartbeat	Запрос состояния соединения (HEARTBEAT, код 4)
heartbeat-ack	Подтверждение запроса проверки состояния соединения (HEARTBEAT ACK, код 5)
init	Инициализация (INIT, код 1)
init-ack	Подтверждение инициализации (INIT ACK, код 2)
sack	Частичное подтверждение (SACK, код 3)
shutdown	Закрытие ассоциации (SHUTDOWN, код 7)
shutdown-ack	Подтверждение закрытия ассоциации (SHUTDOWN ACK, код 8)
shutdown-complete	Окончание закрытия ассоциации (SHUTDOWN COMPLETE, код 14)

Одновременно можно задать более одно типа блоков.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать параметры протокола SCTP для проверки соответствия правилу фильтрации.

Предварительно должен быть определен протокол SCTP при помощи команды *filter <имя> rule <номер_правила> protocol sctp.*

Форма **set** используется для включения фильтрации по протоколу SCTP и указания параметров.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.42 filter <имя> rule <номер_правила> source address <адрес>

Указание адреса отправителя для проверки соответствия в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя>  rule <номер_правила> source address <адрес>
delete filter <имя>  rule <номер_правила> source address <адрес>
show filter <имя>  rule <номер_правила> source address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      source {
         address адрес
     }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

адрес

Адрес отправителя, используемый для проверки соответствия. Поддерживаемые значения приведены в таблице ниже.

Таблица 86 - Поддерживаемые значения адреса отправителя

Значение	Описание
<x.x.x.x>	Адрес IPv4
<x.x.x.x/x>	Подсеть IPv4 (значение 0.0.0.0/0 соответствует любой сети)
<x.x.x.x>-<x.x.x.x>	Диапазон IPv4-адресов
!<x.x.x.x>	Соответствие будет установлено для всех IPv4-адресов, кроме указанного
!<x.x.x.x/x>	Соответствие будет установлено для всех IPv4-адресов, кроме указанной подсети
!<x.x.x.x>-<x.x.x.x>	Соответствие будет установлено для всех IPv4-адресов, кроме адресов, входящих в указанный диапазон

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать адрес отправителя в правиле фильтрации трафика IPv4.

В том случае если явно указаны адрес и номер порта, для пакета устанавливается соответствие критериям правила в том и только том случае, если совпадает как адрес, так и номер порта.

ПРИМЕЧАНИЕ Для указания адреса отправителя адрес задается либо данной командой, либо указанием группы адресов командой filter <имя> rule <номер_правила> source address-group <имя_группы>. Параллельное использование обоих механизмов не допускается.

Форма **set** данной команды используется для указания адреса отправителя в правиле фильтрации трафика.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.43 filter <имя> rule <номер_правила> source address-group <имя_группы>

Указание группы адресов для проверки соответствия IP-адреса отправителя сетевого пакета в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> source address-group <имя_группы>
delete filter <имя> rule <номер_правила> source address-group <имя_группы>
show filter <имя> rule <номер_правила> source address-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
    rule номер_правила {
        source {
            address-group имя_группы
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

имя_группы

Имя группы IPv4-адресов.

Таблица 87 - Допустимые значения для группы адресов

Значение	Описание
<text>	Имя группы
!<text>	Все группы кроме указанной

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет использовать заранее определенную группу адресов для сопоставления с IPv4-адресом отправителя пакета. Группа должна быть предварительно определена при помощи команды *groups address-group <имя_группы>*. Может быть указана только одна группа.

Соответствие для пакета устанавливается в том случае, если IP-адрес совпадает с одним из адресов, входящих в состав указанной группы.

ПРИМЕЧАНИЕ Для указания адреса отправителя адрес задается либо указанием группы адресов данной командой, либо указанием адресов командой filter <имя> rule <номер_правила> source address <адрес>. Параллельное использование обоих механизмов не допускается.

Форма **set** данной команды используется для указания группы адресов отправителя для проверки соответствия.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.44 filter <имя> rule <номер_правила> source address-type <тип>

Указание типа адреса отправителя, по которому будет осуществляться проверка соответствия в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя>  rule <номер_правила> source address-type <тип>
delete filter <имя>  rule <номер_правила> source address-type<тип>
show filter <имя>  rule <номер_правила> source address-type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
     source {
         address-type тип
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

тип

Тип адреса отправителя (источника). Данное правило будет применено к пакетам, тип адреса отправителя (источника) которых соответствует указанному. Допустимые значения приведены в таблице ниже.

Таблица 88 - Допустимые значения типа адреса отправителя

Значение	Описание

unspec	Неопределённый адрес (0.0.0.0)
unicast	Однонаправленный адрес
local	Локальный адрес
broadcast	Широковещательный адрес
multicast	Мультивещательный адрес
anycast	Близковещательный адрес (anycast)
blackhole	Адрес подпадающий под маршрут типа "чёрная дыра"
unreachable	Недостижимый адрес
prohibit	Административно запрещённый для маршрутизации адрес
nat	Преобразуемый сетевой адрес

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать тип адреса отправителя в правиле фильтрации трафика IPv4.

Форма **set** данной команды используется для создания настройки типа адреса источника для правила фильтрации трафика.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.45 filter <имя> rule <номер_правила> source country <код_страны>

Указание двухзначного кода страны отправителя в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> source country <код_страны>
delete filter <имя> rule <номер_правила> source country <код_страны>
show filter <имя> rule <номер_правила> source country
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      source {
         country код_страны
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

код_страны

Двузначный код страны отправителя.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания двухзначного кода страны отправителя в правиле фильтрации трафика IPv4. В одном правиле фильтрации может быть задано не более 15 стран.

ПРИМЕЧАНИЕ Необходимо иметь в виду, что данные о принадлежности IP диапазона к определенному региону берутся из общедоступных источников и могут не обладать 100% точностью. Для дополнения/исключения диапазонов рекомендуется использовать группы IP адресов (groups address-group) в правилах фильтрации.

Форма **set** данной команды используется для указания двухзначного кода страны источника в правиле фильтрации трафика IPv4.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для просмотра настройки.

16.2.46 filter <имя> rule <номер_правила> source domain-group <имя_группы>

Указание группы доменов для проверки соответствия домена отправителя сетевого пакета в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> source domain-group <имя_группы>
delete filter <имя> rule <номер_правила> source domain-group <имя_группы>
show filter <имя> rule <номер_правила> source domain-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
    rule номер_правила {
        source {
            domain-group имя_группы
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

имя_группы

Имя группы доменов.

Таблица 89 - Допустимые значения для группы доменов

Значение	Описание
<text>	Имя группы
!<text>	Все группы кроме указанной

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет использовать заранее определенную группу доменов для сопоставления с доменом отправителя пакета. Группа должна быть предварительно определена при помощи команды *groups domain-group <имя_группы>*. Может быть указана только одна группа.

Соответствие для пакета устанавливается в том случае, если домен совпадает с одним из доменов, входящих в состав указанной группы.

Форма **set** данной команды используется для указания группы доменов отправителя для проверки соответствия.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.47 filter <имя> rule <номер_правила> source ldap

Указание имени пользователя и(или) группы LDAP для проверки соответствия в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> source ldap [group <имя_группы>| user <имя_пользователя>]
delete filter <имя> rule <номер_правила> source ldap [group | user]
show filter <имя> rule <номер_правила> source ldap [group | user]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
    rule номер_правила {
        source {
            ldap {
                group имя_группы
                user имя_пользователя
            }
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

имя_группы

Данное правило будет применено к пакетам, отправителем которых являются клиент VPN PPTP/L2TP, который был аутентифицирован на основе учетной записи пользователя LDAP, входящего в указанную группу.

имя_пользователя

Данное правило будет применено к пакетам, отправителем которых является клиент VPN PPTP/L2TP, который был аутентифицирован на основе учетной записи пользователя LDAP с указанным именем.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать имя пользователя и(или) группы LDAP, для тех случаев когда отправителем является клиент PPTP/L2TP, который был аутентифицирован на основе учетной записи пользователя LDAP с указанным именем.

Форма **set** данной команды используется для создания настройки отправителя для правила фильтрации трафика.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.48 filter <имя> rule <номер_правила> source local-group <имя_группы>

Указание локальной группы МЭ для проверки соответствия в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> source local-group <имя_группы>
delete filter <имя> rule <номер_правила> source local-group <имя_группы>
show filter <имя> rule <номер_правила> source local-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      source {
         local-group имя_группы
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

имя_группы

Имя локальной группы МЭ. Допустимые значения представлены в таблице ниже.

Таблица 90 - Допустимые значения для локальной группы

Значение	Описание
<text>	Имя группы
!<text>	Все группы кроме указанной

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать локальную группу МЭ для сопоставления в правиле фильтрации трафика IPv4.

Форма **set** данной команды используется для указания локальной группы МЭ в правиле фильтрации трафика IPv4.

Форма **delete** данной команды используется для удаления локальной группы МЭ в правиле фильтрации трафика IPv4.

Форма **show** данной команды используется для отображения настройки локальной группы МЭ в правиле фильтрации трафика IPv4.

ПРИМЕЧАНИЕ При использовании политикой фильтра с заданными локальными пользователями/группами, такая политика может быть использована только в качестве системной.

16.2.49 filter <имя> rule <номер_правила> source local-user <имя_пользователя>

Указание локального пользователя МЭ для проверки соответствия в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> source local-user <имя_пользователя>
delete filter <имя> rule <номер_правила> source local-user <имя_пользователя>
show filter <имя> rule <номер_правила> source local-user
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      source {
         local-user имя_пользователя
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

мя_пользователя

Имя локального пользователя МЭ. Допустимые значения представлены в таблице ниже.

Таблица 91 - Допустимые значения для локального пользователя

Значение	Описание
<text>	Имя пользователя
!<text>	Все пользователи кроме указанного

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать локального пользователя МЭ для сопоставления в правиле фильтрации трафика IPv4.

Форма **set** данной команды используется для указания локального пользователя МЭ в правиле фильтрации трафика IPv4.

Форма **delete** данной команды используется для удаления локального пользователя МЭ в правиле фильтрации трафика IPv4.

Форма **show** данной команды используется для отображения настройки локального пользователя МЭ в правиле фильтрации трафика IPv4.

ПРИМЕЧАНИЕ При использовании политикой фильтра с заданными локальными пользователями/группами, такая политика может быть использована только в качестве системной.

16.2.50 filter <имя> rule <номер_правила> source mac-address <mac-адрес>

Указание MAC-адреса отправителя, по которому будет осуществляться проверка соответствия в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> source mac-address <mac-адрес>
delete filter <имя> rule <номер_правила> source mac-address <mac-адрес>
show filter <имя> rule <номер_правила> source mac-address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
    rule номер_правила {
        source {
            mac-address mac-адрес
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

mac-адрес

MAC-адрес для проверки соответствия. Адрес указывается в формате шести разделенных двоеточиями 8-битных шестнадцатеричных чисел, например, 18:31:bf:3c:0d:67.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать MAC-адрес источника, по которому будет осуществляться проверка соответствия пакета критериям правила фильтрации трафика.

Форма **set** данной команды используется для указания MAC-адреса отправителя в правиле фильтрации трафика.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.51 filter <имя> rule <номер_правила> source network-group <имя_группы>

Данный узел команд присутствует в системе для обеспечения обратной совместимости со старыми

версиями оборудования. Вместо него следует использовать функционал filter <имя> rule <номер_правила> source address-group <имя_группы>.

16.2.52 filter <имя> rule <номер_правила> source port <порт>

Указание номера сетевого порта отправителя для проверки соответствия в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> source port <порт>
delete filter <имя> rule <номер_правила> source port <порт>
show filter <имя> rule <номер_правила> source port
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      source {
         port порт
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

порт

Порт отправителя для проверки соответствия. Допустимые значения представлены в таблице ниже:

Таблица 92 – Формат указания порта получателя

Значение	Описание
<text>	Имя порта (любое из файла /etc/services)
<0-65535>	Номер порта
<start>-<end>	Диапазон портов

Возможно также задание списка через запятую, например: "22,telnet,http,123,1001-1005".

Возможно также задание инвертированного списка с помощью "!", например: "!22,telnet,http,123,1001-1005".

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать номера сетевого порта отправителя в правиле фильтрации трафика IPv4. Сетевой порт может быть указан только для протоколов TCP, UDP, SCTP и DCCP. Предварительно должен быть определен протокол при помощи команды *filter <имя> rule <номер_правила> protocol <протокол>*.

В том случае если явно указаны адрес и номер порта, для пакета устанавливается соответствие критериям правила в том и только том случае, если совпадает как адрес, так и номер порта.

ПРИМЕЧАНИЕ Для указания порта отправителя порт задается либо данной командой, либо указанием группы портов командой filter <имя> rule <номер_правила> source port-group <имя_группы>. Параллельное использование обоих механизмов не допускается.

Форма **set** данной команды используется для указания порта отправителя в правила фильтрации трафика IPv4.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.53 filter <имя> rule <номер_правила> source port-group <имя_группы>

Указание группы портов для проверки соответствия порта отправителя сетевого пакета в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила>  source port-group <имя_группы>
delete filter <имя> rule <номер_правила>  source port-group <имя_группы>
show filter <имя> rule <номер_правила>  source port-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      source {
         port-group имя_группы
      }
  }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

имя_группы

Имя группы портов.

Таблица 93 - Допустимые значения для группы портов

Значение	Описание
<text>	Имя группы
!<text>	Все группы кроме указанной

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет использовать заранее определенную группу портов для сопоставления с номером порта отправителя пакета. Группа должна быть предварительно определена при помощи команды *groups port-group <имя_группы>*. Может быть указана только одна группа.

Соответствие для пакета устанавливается в том случае, если номер порта источника (отправителя) пакета совпадает с одним из портов, входящих в состав указанной группы.

ПРИМЕЧАНИЕ Для указания порта отправителя порт задается либо указанием группы портов данной командой, либо указанием портов командой filter <имя> rule <номер_правила> source port <порт>. Параллельное использование обоих механизмов не допускается.

Форма **set** данной команды используется для указания группы портов отправителя для проверки соответствия.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.54 filter <имя> rule <номер_правила> state

Указание состояний соединений, к которым применяется правило фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> state [established <состояние> | invalid <состояние> | new <состояние> | related <состояние>]

delete filter <имя> rule <номер_правила> state [established | invalid | new | related]

show filter <имя> rule <номер_правила> state
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
    rule номер_правила {
        state {
            established состояние
            invalid состояние
            new состояние
            related состояние
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

established *состояние*

Позволяет указать, следует ли применять данное правило к пакетам установленных соединений. Поддерживаются следующие значения:

enable: Применить правило к пакетам установленных соединений;

disable: Не применять правило к пакетам установленных соединений.

invalid *состояние*

Позволяет указать, следует ли применять данное правило к пакетам недействительных соединений. Поддерживаются следующие значения:

enable: Применить правило к пакетам недействительных соединений;

disable: Не применять правила к пакетам недействительных соединений.

new *состояние*

Позволяет указать, следует ли применять данное правило к пакетам новых соединений. Поддерживаются следующие значения:

enable: Применить правило к пакетам новых соединений;

disable: Не применять правило к пакетам новых соединений.

related *состояние*

Позволяет указать, следует ли применять данное правило к пакетам связанных соединений. Поддерживаются следующие значения:

enable: Применить данное правило к пакетам связанных соединений;

disable: Не применять данное правило к пакетам связанных соединений.

Значение по умолчанию

Указанное правило применяется ко всем пакетам вне зависимости от состояния соединения.

Указания по использованию

Данная команда позволяет указать состояния соединений, к пакетам которых будет применяться данное правило фильтрации трафика IPv4.

Established - состояние установленного соединения. Соединение считается установленным в том случае, когда был получен трафик в обоих направлениях.

Invalid - состояние недействительного соединения. Присваивается пакетам, которые не могут быть идентифицированы по каким-либо причинам. Такое возможно в случае нехватки ресурсов системы для обработки пакета; или если пакет не содержит сведений идентифицирующих состояние; или ошибки ICMP, которые не могут быт соотнесены ни с одним известным соединением. Обычно эти пакеты отбрасываются.

New - состояние нового соединения. Такое состояние характерно для пакетов, впервые встреченных системой, содержащих информацию о новом соединении. Для протокола TCP, это пакеты с установленным флагом SYN.

Related - состояние связанного соединения. Такое состояние характерно для соединений, инициированных на основе уже существующего установленного соединения. В качестве примера можно привести соединение для обмена данными протокола FTP, которое будет являться связанным по отношению к установленному управляющему соединению FTP.

Форма **set** данной команды позволяет указать тип пакетов, к которому будет применяться правило фильтрации трафика IPv4.

Форма **delete** данной команды позволяет восстановить поведение, принятое по умолчанию.

Форма **show** данной команды используется для отображения настройки.

ПРИМЕЧАНИЕ При наличии в конфигурации данного фильтра на устройстве производится дефрагментация пакетов. В таком случае фильтр соответствия фрагментированным пакетам fragment не будет отрабатывать корректно.

16.2.55 filter <имя> rule <номер_правила> string <номер_подстроки> case-insensitive

Не учитывать регистр букв при фильтрации по подстрокам в IPv4-пакете.

Синтаксис

```
set filter <имя> rule <номер_правила> string <номер_подстроки> case-insensitive
```

```
delete filter <имя> rule <номер_правила> string <номер_подстроки>case-insensitive
```

```
show filter <имя> rule <номер_правила> string <номер_подстроки>case-insensitive
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      string номер_подстроки {
         case-insensitive
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

номер_подстроки

Множественный узел. Численный идентификатор подстроки. Для установки соответствия на основе нескольких подстрок, следует создать соответствующее количество узлов **string** в одном правиле фильтра трафика, в этом случае соответствие будет установлено только для пакетов, в которых будут обнаружены все указанные подстроки.

case-insensitive

При указании данного параметра поиск будет осуществляться без учета регистра букв в подстроке.

Значение по умолчанию

По умолчанию регистр букв учитывается.

Указания по использованию

При использовании этой команды при поиске подстроки в пакете IPv4 не учитывается регистр букв. Предварительно должна быть определена искомая подстрока при помощи команды *filter <имя> rule <номер_правила> string <номер_подстроки> match <подстрока>* или в шестнадцатеричной нотации при помощи команды *filter <имя> rule <номер_правила> string <номер_подстроки> hex-match <подстрока>*.

Форма **set** данной команды позволяет указать, что требуется не учитывать регистр букв при поиске подстроки.

Форма **delete** данной команды позволяет восстановить поведение, принятое по умолчанию.

Форма **show** данной команды используется для отображения настройки.

16.2.56 filter <имя> rule <номер_правила> string <номер_подстроки> from <смещение>

Установка смещения в пакете IPv4, начиная с которого будет осуществляться поиск подстроки.

Синтаксис

```
set filter <имя> rule <номер_правила> string <номер_подстроки> from <смещение>

delete filter <имя> rule <номер_правила> string <номер_подстроки> from <смещение>

show filter <имя> rule <номер_правила> string номер_подстроки from
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      string номер_подстроки {
         from смещение
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

номер_подстроки

Множественный узел. Численный идентификатор подстроки. Для установки соответствия на основе нескольких подстрок, следует создать соответствующее количество узлов **string** в одном правиле фильтра трафика, в этом случае соответствие будет установлено только для пакетов, в которых будут обнаружены все указанные подстроки.

смещение

Смещение в байтах от начала пакета IPv4. Значение должно находиться в диапазоне от 0 до 65535.

Значение по умолчанию

По умолчанию установлено значение 0, поиск подстроки осуществляется от начала пакета IPv4.

Указания по использованию

Данная команда позволяет указать смещение в пакете IPv4, начиная от которого, будет осуществляться поиск подстроки. Предварительно должна быть определена искомая подстрока при помощи команды *filter <имя> rule <номер_правила> string <номер_подстроки> match <подстрока>* или в шестнадцатеричной нотации при помощи команды *filter <имя> rule <номер_правила> string <номер_подстроки> hex-match <подстрока>*.

Смещение, до которого осуществляется поиск, указывается при помощи команды *filter <имя> rule <номер_правила> string <номер_подстроки> to <смещение>*.

Форма **set** данной команды позволяет указать смещение в пакете IPv4, начиная с которого будет осуществляться поиск подстроки в пакете IPv4.

Форма **delete** данной команды позволяет удалить настройку и восстановить значение, принятое по умолчанию.

Форма **show** данной команды используется для отображения настройки.

16.2.57 filter <имя> rule <номер_правила> string <номер_подстроки> hex-match <подстрока>

Указание подстроки для поиска в шестнадцатеричном виде.

Синтаксис

```
set filter <имя>  rule <номер_правила> string <номер_подстроки> hex-match <подстрока>

delete filter <имя>  rule <номер_правила> string <номер_подстроки> hex-match <подстрока>

show filter <имя>  rule <номер_правила> string <номер_подстроки> hex-match
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      string номер_подстроки {
         hex-match подстрока
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

номер_подстроки

Множественный узел. Численный идентификатор подстроки. Для установки соответствия на основе нескольких подстрок, следует создать соответствующее количество узлов **string** в одном правиле фильтра трафика, в этом случае соответствие будет установлено только для пакетов, в которых будут обнаружены все указанные подстроки.

подстрока

Подстрока для поиска в пакете IPv4. Значение указывается в следующем формате: *текст|xx xx|текст*, где шестнадцатеричное значение ограничено символом ' | ', а шестнадцатеричные блоки (xx), представляющие байт данных, могут быть разделены пробелами, например, |40 41 42 43|. Значение *текст|xx xx|текст* необходимо заключить либо в одинарные (*'текст|xx xx|текст'*), либо в двойные (*"текст|xx xx|текст"*) кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет задать критерий соответствия для пакетов на основе подстроки для поиска в пакете IPv4, значение которой указывается в шестнадцатеричном виде.

Форма **set** данной команды позволяет указать значение подстроки для поиска в шестнадцатеричном виде.

Форма **delete** данной команды позволяет удалить настройку.

Форма **show** данной команды используется для отображения настройки.

16.2.58 filter <имя> rule <номер_правила> string <номер_подстроки> match <подстрока>

Указание подстроки для поиска.

Синтаксис

```
set filter <имя> rule <номер_правила> string <номер_подстроки> match <подстрока>

delete filter <имя> rule <номер_правила> string <номер_подстроки> match <подстрока>

show filter <имя> rule <номер_правила> string <номер_подстроки> match
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      string номер_подстроки {
         match подстрока
      }
  }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

номер_подстроки

Множественный узел. Численный идентификатор подстроки. Для установки соответствия на основе нескольких подстрок, следует создать соответствующее количество узлов **string** в одном правиле фильтра трафика, в этом случае соответствие будет установлено только для пакетов, в которых будут обнаружены все указанные подстроки.

подстрока

Подстрока для поиска в пакете IPv4.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет задать критерий соответствия для пакетов на основе подстроки для поиска в пакете IPv4. Для того чтобы осуществлять поиск на основе нескольких подстрок, следует для одного правила фильтра трафика указать несколько узлов конфигурации **string**, в этом случае соответствие будет установлено только для пакетов, в которых будут обнаружены все указанные подстроки.

Форма **set** данной команды позволяет указать значение подстроки для поиска.

Форма **delete** данной команды позволяет удалить настройку.

Форма **show** данной команды используется для отображения настройки.

16.2.59 filter <имя> rule <номер_правила> string <номер_подстроки> negation

Установка соответствия на основе отсутствия указанной подстроки в пакете IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> string <номер_подстроки> negation
delete filter <имя> rule <номер_правила> string <номер_подстроки> negation
show filter <имя> rule <номер_правила> string <номер_подстроки> negation
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
```

```
        string номер_подстроки {
            negation
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

номер_подстроки

Множественный узел. Численный идентификатор подстроки. Для установки соответствия на основе нескольких подстрок, следует создать соответствующее количество узлов **string** в одном правиле фильтра трафика, в этом случае соответствие будет установлено только для пакетов, в которых будут обнаружены все указанные подстроки.

Значение по умолчанию

Отсутствует.

Указания по использованию

При указании команды соответствие будет устанавливаться для пакетов, в которых отсутствует указанная подстрока. Предварительно должна быть определена искомая подстрока при помощи команды *filter <имя> rule <номер_правила> string <номер_подстроки> match <подстрока>* или в шестнадцатеричной нотации при помощи команды *filter <имя> rule <номер_правила> string <номер_подстроки> hex-match <подстрока>*.

Форма **set** данной команды позволяет указать, что соответствие будет устанавливаться для пакетов, в которых отсутствует указанная подстрока.

Форма **delete** данной команды позволяет удалить настройку.

Форма **show** данной команды используется для отображения настройки.

16.2.60 filter <имя> rule <номер_правила> string <номер_подстроки> to <смещение>

Установка смещения в пакете IPv4, до которого будет осуществляться поиск подстроки.

Синтаксис

```
set filter <имя> rule <номер_правила> string <номер_подстроки> to <смещение>
delete filter <имя> rule <номер_правила> string <номер_подстроки> to <смещение>
show filter <имя> rule <номер_правила> string <номер_подстроки> to
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
    rule номер_правила {
        string номер_подстроки {
            to смещение
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

номер_подстроки

Множественный узел. Численный идентификатор подстроки. Для установки соответствия на основе нескольких подстрок, следует создать соответствующее количество узлов **string** в одном правиле фильтра трафика, в этом случае соответствие будет установлено только для пакетов, в которых будут обнаружены все указанные подстроки.

смещение

Смещение в байтах от начала пакета IPv4. Значение должно находиться в диапазоне от 0 до 65535.

Значение по умолчанию

По умолчанию поиск подстроки осуществляется до конца пакета IPv4.

Указания по использованию

Данная команда позволяет указать смещение в пакете IPv4, до которого, будет осуществляться поиск подстроки. Предварительно должна быть определена искомая подстрока при помощи команды *filter <имя> rule <номер_правила> string <номер_подстроки> match <подстрока>* или в шестнадцатеричной нотации при помощи команды *filter <имя> rule <номер_правила> string <номер_подстроки> hex-match <подстрока>*.

Смещение, от которого начинается поиск, указывается при помощи команды *filter <имя> rule <номер_правила> string <номер_подстроки> from <смещение>*.

Форма **set** данной команды позволяет указать смещение в пакете IPv4, до которого будет осуществляться поиск подстроки в пакете IPv4.

Форма **delete** данной команды позволяет удалить настройку и восстановить значение, принятое по умолчанию.

Форма **show** данной команды используется для отображения настройки.

16.2.61 filter <имя> rule <номер_правила> tcp flags <флаг>

Указание флагов TCP для проверки соответствия в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> tcp flags <флаг>
delete filter <имя> rule <номер_правила> tcp flags
show filter <имя> rule <номер_правила> tcp flags
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
    rule номер_правила {
        tcp {
            flags флаг
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

флаг

Указание флагов TCP для проверки соответствия. Поддерживаются следующие значения: SYN, ACK, FIN, RST, URG, PSH и ALL. При указании нескольких флагов, они должны быть указаны через запятую. Например, при указании "SYN, !ACK, !FIN, !RST" будет установлено соответствие только в том случае, если установлен флаг SYN и не установлены флаги ACK, FIN, RST. Указание ALL может быть использовано для проверки того, что установлены все флаги, указание !ALL используется для проверки того, что не установлено ни одного флага. При указании перед значением флага восклицательного знака ("!") соответствие будет установлено в том случае, если флаг не установлен.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет проверять соответствие сетевых пакетов критериям правила фильтрации трафика IPv4 на основе флагов TCP. Предварительно должен быть определен протокол TCP для правила фильтрации при помощи команды *filter <имя> rule <номер_правила> protocol tcp*.

Форма **set** данной команды используется для указания флагов TCP на основе которых будет осуществляться проверка соответствия.

Форма **delete** данной команды позволяет восстановить поведение по умолчанию.

Форма **show** данной команды позволяет отобразить настройку.

ПРИМЕЧАНИЕ В случае использования фильтра для отсеивания TCP пакетов с некорректными наборами флагов, такой фильтр не будет работать совместно с трансляцией адресов NAT. Так как при включении NAT такие пакеты отбрасываются до применения политик фильтрации.

16.2.62 filter <имя> rule <номер_правила> tcp mss <значение>

Указание максимального размера сегмента для проверки соответствия в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> tcp mss <значение>
delete filter <имя> rule <номер_правила> tcp mss
show filter <имя> rule <номер_правила> tcp mss
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      tcp {
        mss значение
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

значение

Максимальный размер сегмента. Допустимые значения приведены в таблице ниже.

Таблица 94 - Допустимые значения максимального размера сегмента

Значение	Описание
<*x*>	Одиночное значение (где *x* - целое в диапазоне от *0* до *65535*)
<*x*>-<*y*>	Диапазон значений (где *x, y* - целое в диапазоне от *0* до *65535*, *x* < *y*)

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет проверять соответствие сетевых пакетов IPv4 критериям правила на основе указанного максимального размера сегмента. Предварительно должен быть определен протокол TCP для правила фильтрации при помощи команды *filter <имя> rule <номер_правила> protocol tcp*.

Форма **set** данной команды используется для указания максимального размера сегмента, на основе которых будет осуществляться проверка соответствия.

Форма **delete** данной команды позволяет восстановить поведение по умолчанию.

Форма **show** данной команды позволяет отобразить установленное в текущий момент значение максимального размера сегмента.

16.2.63 filter <имя> rule <номер_правила> tcp option <опция>

Указание опции TCP для проверки соответствия в правиле фильтрации трафика IPv4.

Синтаксис

```
set filter <имя> rule <номер_правила> tcp option <опция>
delete filter <имя> rule <номер_правила> tcp option
show filter <имя> rule <номер_правила>  tcp option
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      tcp {
         option опция
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

опция

Проверка на наличие/отсутствие указанной опции TCP в пакете. Допустимые значения приведены в таблице ниже.

Таблица 95 - Допустимые значения опции TCP

Значение	**Описание**
<x>	Номер опции TCP (где *x* - целое в диапазоне от *1* до *255*)
md5	Имитовставка с использованием алгоритма MD5 (номер 19)
mss	Максимальный размер сегмента (номер 2)
sack-permitted	Разрешение выборочного подтверждения (номер 4)
sack	Выборочное подтверждение (номер 5)
timestamp	Временная отметка (номер 8)
wscale	Масштабирование окна (номер 3)
!<y>	Проверка отсутствия заданной опции (*<y>* - любое значение, приведенное выше)

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет проверять наличие/отсутствие в сетевых пакетах указанной опции TCP. Предварительно должен быть определен протокол TCP для правила фильтрации при помощи команды *filter <имя> rule <номер_правила> protocol tcp*.

Форма **set** данной команды используется для указания опции, на основании которой будет осуществляться проверка соответствия.

Форма **delete** данной команды позволяет удалить заданное значение опции.

Форма **show** данной команды позволяет отобразить установленное в текущий момент значение проверяемой опции.

16.2.64 filter <имя> rule <номер_правила> time

Применение правил фильтрации трафика с учетом даты и времени.

Синтаксис

```
set filter <имя> rule <номер_правила> time [monthdays <дни_месяца> | startdate <дата> | starttime <время> | stopdate <дата> | stoptime <время>| utc | weekdays <дни_недели>]
```

```
delete filter <имя> rule <номер_правила> time
```

```
show filter <имя> rule <номер_правила> time
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
  rule номер_правила {
      time {
         monthdays дни_месяца
         startdate дата
         starttime время
         stopdate дата
         stoptime время
         utc
```

```
            weekdays дни_недели
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

дни_месяца

Дни месяца, в которые применяется указанное правило. Поддерживаются следующие значения: дни месяца (с 1 по 31), указанные через запятую (например, *3,15,24*). Может быть указан восклицательный знак ("!") для указания отрицания списка значений (например, *!3,15,24*). В данном случае правило фильтрации трафика будет применяться ежедневно, кроме указанных дней месяца.

startdate *дата*

Дата (и, в случае необходимости, время) начала периода действия правила. Указывается в следующем формате:

- **гггг-мм-дд** (например, 2020-04-21);
- **гггг-мм-ддТчч:мм:сс** (время, при необходимости указания, отделяется символом "T", например, 2020-04-21T16:45:00).

Время указывается в 24-часовом формате (значение должно находиться в диапазоне от 00:00:00 до 23:59:59). В том случае если время явно не указано, по умолчанию устанавливается начало указанного дня (т.е., 00:00:00). Для указания окончания периода действия правила используется параметр **stopdate**.

starttime *время*

Время начала периода, в течение которого правило будет применяться. Указывается в следующем формате:

- **чч:мм:сс** (например, 16:45:00).

Время указывается в 24-часовом формате (значение должно находиться в диапазоне от 00:00:00 до 23:59:59). Для указания времени окончания периода действия правила используется параметр **stoptime**.

stopdate *дата*

Дата (и, в случае необходимости, время) окончания периода действия правила. Указывается в следующем формате:

- **гггг-мм-дд** (например, 2020-04-21);
- **гггг-мм-ддТчч:мм:сс** (время, при необходимости указания, отделяется символом "T", например, 2020-04-21T16:45:00).

Время указывается в 24-часовом формате (значение должно находиться в диапазоне от 00:00:00 до 23:59:59). В том случае если время явно не указано, по умолчанию устанавливается начало указанного дня (т.е., 00:00:00). Для указания начала периода действия правила используется параметр **startdate**.

stoptime *время*

Время окончания периода, в течение которого правило будет применяться. Указывается в следующем формате:

- **чч:мм:сс** (например, 16:45:00).

Время указывается в 24-часовом формате (значение должно находиться в диапазоне от 00:00:00 до 23:59:59). Для указания времени начала периода действия правила используется параметр **starttime**.

utc

При указании данного параметра время, заданное при помощи параметров **startdate**, **stopdate**, **starttime**, и **stoptime**, должно быть интерпретировано как время UTC, а не как местное время.

дни_недели

Дни недели, по которым указанное правило будет применяться. Поддерживаются следующие значения: **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat** и **Sun**.

Дни недели могут быть указаны через запятую (например: **Mon**,**Wed**,**Fri**).

Для указания отрицания списка значений может быть указан восклицательный знак "!" (например, **!Mon**,**Wed**,**Fri**). В данном случае правило фильтрации трафика будет применяться ежедневно, кроме указанных дней недели.

Значение по умолчанию

Правило применяется постоянно без учета даты и времени.

Указания по использованию

Данная команда используется для ограничения времени, в течение которого применяется указанное правило фильтрации трафика.

Все параметры являются необязательными. В случае указания нескольких параметров объединяются логическим И.

Форма **set** данной команды используется для указания периода действия правила фильтрации трафика IPv4.

Форма **delete** данной команды используется для восстановления поведения по умолчанию.

Форма **show** данной команды используется для отображения настройки периода действия правила фильтрации трафика.

16.2.65 filter <имя> rule <номер_правила> ttl <значение>

Применение правил фильтрации трафика с учетом времени жизни пакетов.

Синтаксис

```
set filter <имя> rule <номер_правила> ttl <значение>
delete filter <имя> rule <номер_правила> ttl
show filter <имя> rule <номер_правила> ttl
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      ttl {
         значение
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

значение

Значение знака сравнения и время жизни пакета. Допустимые значения приведены в таблице ниже.

Таблица 96 - Допустимые значения правила фильтрации трафика на основе времени жизни пакетов

Значение	Описание
equals <x>	Применение правила к пакетам, время жизни которых равно указанному (где *x* - целое в диапазоне от *0* до *255*)
greater-than <x>	Применение правила к пакетам, время жизни которых больше указанного (где *x* - целое в диапазоне от *0* до *254*)
less-than <x>	Применение правила к пакетам, время жизни которых меньше указанного (где *x* - целое в диапазоне от *1* до *255*)
not-equals <x>	Применение правила к пакетам, время жизни которых не равно указанному (где *x* - целое в диапазоне от *0* до *255*)

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет проверять соответствие сетевых пакетов критериям правила на основе времени жизни пакетов.

Форма **set** данной команды используется для создания правила фильтрации, основанного на времени жизни пакетов.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

ПРИМЕЧАНИЕ Межсетевой экран уменьшает значение ttl для транзитного трафика (in/out) перед фильтрацией. Для трафика, предназначенного самому устройству (направление local) значение ttl не уменьшается.

16.2.66 filter-ipv6 <имя>

Указание имени фильтра трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя>
delete filter-ipv6 <имя>
show filter-ipv6 <имя>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {}
```

Параметры

имя

Имя фильтра трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать имя фильтра трафика. Следует отметить,что при создании пустого узла **filter-ipv6** (без правил) трафик IPv6 им обрабатываться не будет. Настройка узла **filter-ipv6** не влияет на трафик IPv4.

Форма **set** данной команды используется для указания имени фильтра трафика.

Форма **delete** данной команды используется для удаления фильтра трафика с заданным именем.

Форма **show** данной команды используется для отображения фильтра трафика.

16.2.67 filter-ipv6 <имя> description <описание>

Указание краткого описания для фильтра трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> description <описание>
delete filter-ipv6 <имя> description
show filter-ipv6 <имя> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   description описание
}
```

Параметры

имя

Имя фильтра трафика.

описание

Описание фильтра трафика. Если текст описания фильтра трафика не содержит пробелов, то *описание* не требует использования дополнительных символов, иначе *описание* заключается либо в одинарные (*'описание'*), либо в двойные (*"описание"*) кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать описание для фильтра трафика IPv6.

Форма **set** данной команды используется для создания и изменения описания.

Форма **delete** данной команды используется для удаления описания.

Форма **show** данной команды используется для отображения настройки описания.

16.2.68 filter-ipv6 <имя> rule <номер_правила>

Определение правила указанного фильтра трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила>
delete filter-ipv6 <имя> rule <номер_правила>
show filter-ipv6 <имя> rule <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно находиться в диапазоне от 1 до 9999. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации **rule**.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет определить правило определённого фильтра трафика IPv6. Определённый фильтр трафика может включать в себя до 9999 настраиваемых правил. Правила в фильтре трафика в порядке следования их номеров, от наименьшего к наибольшему. Напрямую изменить номер правила нельзя, так как он является идентификатором узла конфигурации; однако, можно изменять номера правил при помощи команды **rename**. Для того чтобы не прибегать к изменению номеров правил, хорошей практикой является указание номеров с шагом 10. Это позволяет оставить пространство, куда можно будет впоследствии добавить новые правила.

Следует отметить, что при создании правила соответствия без уточняющих параметров, весь трафик IPv6 будет попадать под его действие.

Форма **set** данной команды используется для создания или изменения правила определённого фильтра трафика.

Форма **delete** данной команды используется для удаления правила из фильтра трафика.

Форма **show** данной команды используется для отображения настройки правила фильтра трафика.

16.2.69 filter-ipv6 <имя> rule <номер_правила> 32bits

Сопоставление 32-битных слов внутри пакета.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> 32bits
delete filter-ipv6 <имя> rule <номер_правила> 32bits
show filter-ipv6 <имя> rule <номер_правила> 32bits
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      32bits {
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать сопоставление 32-битных слов внутри пакета.

Форма **set** данной команды используется для создания сопоставления.

Форма **delete** данной команды используется для удаления сопоставления.

Форма **show** данной команды используется для отображения настройки сопоставления.

16.2.70 filter-ipv6 <имя> rule <номер_правила> 32bits invert

Инверсия сопоставления 32-битных слов внутри пакета.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> 32bits invert
delete filter-ipv6 <имя> rule <номер_правила> 32bits invert
show filter-ipv6 <имя> rule <номер_правила> 32bits
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      32bits {
        invert
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

invert

При указании данного параметра будет осуществляться инверсия сопоставления 32-битных слов внутри пакета.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать инверсию сопоставления 32-битных слов внутри пакета.

Форма **set** данной команды используется для создания инверсии сопоставления.

Форма **delete** данной команды используется для удаления инверсии сопоставления.

Форма **show** данной команды используется для отображения настройки инверсии сопоставления.

16.2.71 filter-ipv6 <имя> rule <номер_правила> 32bits match <параметр_сопоставления> location <адрес>

Задание адреса и преобразования значения сопоставления 32-битных слов внутри пакета.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> 32bits match <параметр_сопоставления> location <адрес>

delete filter-ipv6 <имя> rule <номер_правила> 32bits match <параметр_сопоставления> location <адрес>

show filter-ipv6 <имя> rule <номер_правила> 32bits match <параметр_сопоставления> location
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
     32bits {
        match параметр_сопоставления {
          location адрес
        }
     }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

параметр_сопоставления

Параметр сопоставления. Значение должно находиться в диапазоне от 0 до 4294967295.

адрес

Адрес и преобразования значения. Поддерживаются следующие значения:

Таблица 97 - Допустимые значения поля location

Значение	Описание
<0-4294967295>	Десятичный адрес значения
<0x00000000-0xFFFFFFFF>	Шестнадцатеричный адрес значения
x & y	Маска y (битовое "и") значения x
x << y	Сдвиг значения x влево на y
x >> y	Сдвиг значения x вправо на y
x @ y	Использование значения по смещению y относительно адреса x

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет задать адрес и преобразование значения сопоставления 32-битных слов внутри пакета.

Форма **set** данной команды используется для задания адреса.

Форма **delete** данной команды используется для удаления адреса.

Форма **show** данной команды используется для отображения настройки адреса.

16.2.72 filter-ipv6 <имя> rule <номер_правила> 32bits match <параметр_сопоставления> value <значение>

Задание значения для сопоставления 32-битных слов внутри пакета.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> 32bits match <параметр_сопоставления> value <значение>
```

```
delete filter-ipv6 <имя> rule <номер_правила> 32bits match <параметр_сопоставления> values
```

```
how filter-ipv6 <имя> rule <номер_правила> 32bits match <параметр_сопоставления> value
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      32bits {
         match параметр_сопоставления {
            value значение
         }
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

параметр_сопоставления

Параметр сопоставления. Значение должно находиться в диапазоне от 0 до 4294967295.

значение

Значение для сопоставления. Поддерживаются следующие значения:

Таблица 98 - Допустимые значения поля value

Значение	**Описание**
<0-4294967295>	Десятичное значение
<0x00000000-0xFFFFFFFF>	Шестнадцатеричное значение
<x-y>	Диапазон значений

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет задать значения для сопоставления 32-битных слов внутри пакета.

Форма **set** данной команды используется для задания значения.

Форма **delete** данной команды используется для удаления значения.

Форма **show** данной команды используется для отображения настройки.

16.2.73 filter-ipv6 <имя> rule <номер_правила> description <описание>

Указание краткого описания для правила фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> description <описание>
delete filter-ipv6 <имя> rule <номер_правила> description
show filter-ipv6 <имя> rule <номер_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      description описание
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

описание

Краткое описание правила. Если текст описания правила не содержит пробелов, то *описание* не требует использования дополнительных символов, иначе *описание* заключается либо в одинарные (*'описание'*), либо в двойные (*"описание"*) кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать краткое описание для правила фильтрации трафика определённого фильтра.

Форма **set** данной команды используется для создания описания.

Форма **delete** данной команды используется для удаления описания.

Форма **show** данной команды используется для отображения настройки описания.

16.2.74 filter-ipv6 <имя> rule <номер_правила> destination address <адрес>

Указание адреса получателя для проверки соответствия в правиле фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила>destination address <адрес>
```

```
delete filter-ipv6 <имя> rule <номер_правила>destination address <адрес>
show filter-ipv6 <имя> rule <номер_правила>destination address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      destination {
         address адрес
     }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

адрес

Адрес получателя, используемый для проверки соответствия. Поддерживаемые значения приведены в таблице ниже.

Таблица 99. Поддерживаемые значения адреса получателя

Значение	**Описание**
<h:h:h:h:h:h:h:h>	Адрес IPv6
<h:h:h:h:h:h:h:h/x>	Подсеть IPv6 (значение ::/0 соответствует любой сети)
<h:h:h:h:h:h:h:h>-<h:h:h:h:h:h:h:h>	Диапазон IPv6-адресов
!<h:h:h:h:h:h:h:h>	Соответствие будет установлено для всех IPv6-адресов, кроме указанного
!<h:h:h:h:h:h:h:h/x>	Соответствие будет установлено для всех IPv6-адресов, кроме указанной подсети
!<h:h:h:h:h:h:h:h>-<h:h:h:h:h:h:h:h>	Соответствие будет установлено для всех IPv6-адресов, кроме адресов, входящих в указанный диапазон

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать адрес получателя в правиле фильтрации трафика IPv6.

В том случае если явно указаны адрес и номер порта, для пакета устанавливается соответствие критериям правила в том и только том случае, если совпадает как адрес, так и номер порта.

Форма **set** данной команды позволяет указать или изменить адрес получателя.

Форма **delete** данной команды позволяет удалить настройку адреса получателя.

Форма **show** данной команды позволяет отобразить настройку адреса получателя.

16.2.75 filter-ipv6 <имя> rule <номер_правила> destination address-type <тип>

Указание типа адреса получателя, по которому будет осуществляться проверка соответствия в правиле фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> destination address-type <тип>
delete filter-ipv6 <имя> rule <номер_правила> destination address-type <тип>
show filter-ipv6 <имя> rule <номер_правила> destination address-type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      destination {
         address-type тип
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

тип

Тип адреса получателя (назначения). Данное правило будет применено к пакетам, тип адреса получателя (назначения) которых соответствует указанному. Допустимые значения приведены в таблице ниже.

Таблица 100 - Допустимые значения типа адреса получателя

Значение	Описание
unspec	Неопределённый адрес (::)
unicast	Однонаправленный адрес
local	Локальный адрес
multicast	Мультивещательный адрес
anycast	Близковещательный адрес (anycast)
unreachable	Недостижимый адрес

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать тип адреса получателя в правиле фильтрации трафика IPv6.

Форма **set** данной команды используется для создания настройки типа адреса назначения для правила фильтрации трафика.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.76 filter-ipv6 <имя> rule <номер_правила> destination country <код_страны>

Указание двухзначного кода страны получателя в правиле фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> destination country <код_страны>
```

```
delete filter-ipv6 <имя> rule <номер_правила> destination country <код_страны>
show filter-ipv6 <имя> rule <номер_правила> destination country
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
    rule номер_правила {
        destination {
            country код_страны
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

код_страны

Двузначный код страны получателя.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания двухзначного кода страны получателя в правиле фильтрации трафика IPv6. В одном правиле фильтрации может быть задано не более 15 стран.

ПРИМЕЧАНИЕ Необходимо иметь в виду, что данные о принадлежности IP диапазона к определенному региону берутся из общедоступных источников и могут не обладать 100% точностью. Для дополнения/исключения диапазонов рекомендуется использовать группы IP адресов (***groups address-group***) в правилах фильтрации.

Форма **set** данной команды используется для указания двухзначного кода страны получателя в правиле фильтрации трафика.

Форма **delete** данной команды используется для удаления настройки двухзначного кода страны получателя в правиле фильтрации трафика.

Форма **show** данной команды используется для просмотра настройки двухзначного кода страны получателя в правиле фильтрации трафика.

16.2.77 filter-ipv6 <имя> rule <номер_правила> destination port <порт>

Указание номера сетевого порта получателя для проверки соответствия в правиле фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> destination port <порт>
delete filter-ipv6 <имя> rule <номер_правила> destination port <порт>
show filter-ipv6 <имя> rule <номер_правила> destination port
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      destination {
         port порт
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

порт

Порт получателя для проверки соответствия. Допустимые значения представлены в таблице ниже:

Таблица 101 – Формат указания порта получателя

Значение	Описание
<text>	Имя порта (любое из файла /etc/services)
<0-65535>	Номер порта
<start>-<end>	Диапазон портов

Возможно также задание списка через запятую, например: "22,telnet,http,123,1001-1005".

Возможно также задание инвертированного списка с помощью "!", например: "!22,telnet,http,123,1001-1005".

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать номера сетевого порта получателя в правиле фильтрации трафика IPv6. Может быть указан только для протоколов TCP, UDP, SCTP и DCCP. Предварительно должен быть определен протокол при помощи команды *filter-ipv6 <имя> rule <номер_правила> protocol <протокол>*.

В том случае если явно указаны адрес и номер порта, для пакета устанавливается соответствие критериям правила в том и только том случае, если совпадает как адрес, так и номер порта.

Форма **set** данной команды позволяет указать или изменить номер сетевого порта получателя.

Форма **delete** данной команды позволяет удалить настройку номера сетевого порта получателя.

Форма **show** данной команды позволяет отобразить настройку номера сетевого порта получателя.

16.2.78 filter-ipv6 <имя> rule <номер_правила> disable

Отключение указанного правила фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> disable
delete filter-ipv6 <имя> rule <номер_правила> disable
show filter-ipv6 <имя> rule <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      disable
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

disable

При указании данного параметра будет отключено указанное правило фильтрации трафика.

Значение по умолчанию

Правило включено (используется).

Указания по использованию

Данная команда позволяет отключить правило фильтрации трафика IPv6. Это может быть полезно при проверке того, как фильтр трафика функционирует без указанного правила. При этом не нужно удалять и заново создавать данное правило.

Форма **set** данной команды используется для отключения правила фильтрации трафика.

Форма **delete** данной команды используется для включения правила фильтрации трафика.

Форма **show** данной команды используется для отображения настройки правила фильтрации трафика.

16.2.79 filter-ipv6 <имя> rule <номер_правила> dscp <значение>

Установка соответствия на основе поля DSCP.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> dscp <значение>
delete filter-ipv6 <имя> rule <номер_правила> dscp <значение>
show filter-ipv6 <имя> rule <номер_правила> dscp
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      dscp значение
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

значение

Значение поля DSCP, на основе которого устанавливается соответствие. Допустимые значения приведены в таблице ниже.

Таблица 102 - Допустимые значения поля DSCP

Значение	**Описание**
<x>	Численное значение DSCP (где *x* - десятичное значение в диапазоне от *0* до *63*)
<x>	Численное значение DSCP (где *x* - шестнадцатеричное значения в диапазоне от *0* до *3F* в формате *0xYZ*, например, *0x2E* или *0x2e*)
default	Значение DSCP по умолчанию, соответствующее стандартной пересылке (шестнадцатеричное значение - *0x0*, двоичное значение - *000000*)
EF	Значение Express Forwarding, соответствующее экстренной пересылке
AFxy	Значение Assured Forwarding, соответствующее гарантированной пересылке (*x* находится в диапазоне от *1* до *4*, y - от *1* до *3*)
CSx	Значение Class Selector поддерживает обратную совместимость с полем приоритета IP (*x* находится в диапазоне от *1* до *7*)

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать проверку соответствия на основе поля DSCP.

Форма **set** данной команды позволяет указать проверку соответствия на основе поля DSCP.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.80 filter-ipv6 <имя> rule <номер_правила> ecn ip ect <значение>

Установка соответствия на основе флага ECT в заголовке IP.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> ecn ip ect <значение>
delete filter-ipv6 <имя> rule <номер_правила> ecn ip ect <значение>
show filter-ipv6 <имя> rule <номер_правила> ecn ip ect
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      ecn {
         ip {
            ect значение
         }
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

значение

Значение флага ECT в заголовке IP, на основе которого устанавливается соответствие. Допустимые значения приведены в таблице ниже.

Таблица 103 - Допустимые значения флага ECT

Значение	Описание
<x>	Значение флага ECN (где *x* - целое в диапазоне от *0* до *3*)
!<x>	Все значения флага ECN, кроме указанного (где *x* - целое в диапазоне от *0* до *3*)

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать проверку соответствия на основе значения флага ECT в заголовке IP.

Форма **set** данной команды позволяет указать проверку соответствия на основе значения флага ECT в заголовке IP.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.81 filter-ipv6 <имя> rule <номер_правила> ecn tcp cwr <значение>

Установка соответствия на основе флага CWR в заголовке TCP.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> ecn tcp cwr <значение>
delete filter-ipv6 <имя> rule <номер_правила> ecn tcp cwr <значение>
show filter-ipv6 <имя> rule <номер_правила> ecn tcp cwr
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      ecn {          tcp {
            cwr значение
         }
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

значение

Значение флага CWR в заголовке TCP, на основе которого устанавливается соответствие. Допустимые значения: 0, 1.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать проверку соответствия на основе значения флага CWR в заголовке TCP. Предварительно должен быть определен протокол TCP для правила фильтрации при помощи команды *filter <имя> rule <номер_правила> protocol tcp*.

Форма **set** данной команды позволяет указать проверку соответствия на основе значения флага CWR в заголовке TCP.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.82 filter-ipv6 <имя> rule <номер_правила> ecn tcp ece <значение>

Установка соответствия на основе флага ECE в заголовке TCP.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> ecn tcp ece <значение>
delete filter-ipv6 <имя> rule <номер_правила> ecn tcp ece <значение>
show filter-ipv6 <имя> rule <номер_правила> ecn tcp ece
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      ecn {
         tcp {
            ece значение
         }
      }
  }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

значение

Значение флага ECE в заголовке TCP, на основе которого устанавливается соответствие. Допустимые значения: 0, 1.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать проверку соответствия на основе значения флага ECE в заголовке TCP. Предварительно должен быть определен протокол TCP для правила фильтрации при помощи команды *filter <имя> rule <номер_правила> protocol tcp*.

Форма **set** данной команды позволяет указать проверку соответствия на основе значения флага ECE в заголовке TCP.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.83 filter-ipv6 <имя> rule <номер_правила> exclude

Исключение правила из фильтра.

Синтаксис

```
set filter-ipv6 <имя>rule <номер_правила> exclude
delete filter-ipv6 <имя>rule <номер_правила> exclude
show filter-ipv6 <имя>rule <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      exclude   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет исключать пакеты, удовлетворяющие критериям правила.

Форма **set** данной команды позволяет указать правило, которое необходимо исключить из набора правил фильтра.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

ПРИМЕЧАНИЕ При применении исключения правила трафик, удовлетворяющий критериям такого правила, будет считаться не соответствующим заданному фильтру. Проверка соответствия дальнейшим правилам этого фильтра проводиться не будет.

ПРИМЕЧАНИЕ Следует учитывать, что правило исключения не отменяет соответствие трафика предыдущим правилам фильтра. То есть если трафик удовлетворяет критериям хотя бы одного предыдущего правила, то он считается соответствующим заданному фильтру несмотря на соответствие критериям правила

исключения.

16.2.84 filter-ipv6 <имя> rule <номер_правила> hop-limit <значение>

Применение правил фильтрации трафика с учетом ограничения транзитных узлов.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> hop-limit <значение>
delete filter-ipv6 <имя> rule <номер_правила> hop-limit
show filter-ipv6 <имя> rule <номер_правила> hop-limit
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      hop-limit {
         значение
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

значение

Значение знака сравнения и количество транзитных узлов. Допустимые значения приведены в таблице ниже.

Таблица 104 - Допустимые значения ограничения транзитных узлов

Значение	Описание
equals <x>	Применение правила к пакетам, количество транзитных узлов которых равно указанному (где *x* - целое в диапазоне от *0* до *255*)
greater-than <x>	Применение правила к пакетам, количество транзитных узлов которых больше указанного (где *x* - целое в диапазоне от *0* до *254*)
less-than <x>	Применение правила к пакетам, количество транзитных узлов которых меньше указанного (где *x* - целое в диапазоне от *1* до *255*)
not-equals <x>	Применение правила к пакетам, количество транзитных узлов которых не равно указанному (где *x* - целое в диапазоне от *0* до *255*)

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет проверять соответствие сетевых пакетов критериям правила на основе количества транзитных узлов.

Форма **set** данной команды используется для создания правила фильтрации, основанного на количестве транзитных узлов.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

ПРИМЕЧАНИЕ Межсетевой экран уменьшает значение hop-limit для транзитного трафика (in/out) перед фильтрацией. Для трафика, предназначенного самому устройству (направление local) значение hop-limit не уменьшается.

16.2.85 filter-ipv6 <имя> rule <номер_правила> icmpv6 type <тип>

Указание кода и типа ICMPv6 для правила фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> icmpv6 type <тип>
delete filter-ipv6 <имя> rule <номер_правила> icmpv6 type
show filter-ipv6 <имя> <номер_правила> icmpv6 type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      icmpv6 {
         type тип
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

тип

Корректный тип ICMPv6. Допустимые значения приведены в таблице ниже.

Таблица 105 - Допустимые значения проверки соответствия типов icmp

Значение	Описание
<0-255>	Проверка соответствия по номеру типа сообщения
<0-255>/<0-255>	Проверка соответствия по номеру типа сообщения и код сообщения
<текст>	Проверка соответствия по типу сообщения в текстовом формате (например: network-unreachable)
!<0-255>	Соответствие будет установлено для всех типов сообщений, кроме указанного номера типа сообщения
!<0-255>/<0-255>	Соответствие будет установлено для всех типов сообщений, кроме указанного номера типа и кода сообщения
!<текст>	Соответствие будет установлено для всех типов сообщений, кроме указанного

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет определить типы ICMPv6 сообщений, к которым применяется данное правило, например, эхо-запрос или эхо-ответ. Для пакетов ICMPv6 указанного типа будет установлено соответствие данному правилу. Предварительно должен быть определен протокол ICMPv6 при помощи команды *filter-ipv6 <имя> rule <номер_правила> protocol icmpv6*.

Форма **set** данной команды используется для указания кода и типа ICMPv6 для указанного правила

Форма **delete** данной команды используется для удаления кода или типа ICMPv6 для указанного правила.

Форма **show** данной команды используется для отображения кода или типа ICMPv6 для указанного правила.

16.2.86 filter-ipv6 <имя> rule <номер_правила> ipsec <тип>

Установка соответствия для пакетов IPSec.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> ipsec <тип>
delete filter-ipv6 <имя> rule <номер_правила> ipsec <тип>
show filter-ipv6 <имя> rule <номер_правила> ipsec
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
  rule номер_правила {
      ipsec {
         тип
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

тип

Тип проверки соответствия для входящих пакетов IPSec. Допустимые значения:

match-ipsec: Установка соответствия для пакетов, попадающих под политику IPSec;

match-none: Установка соответствия для пакетов, не попадающих под политику IPSec.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для установки соответствия входящим пакетам IPSec или, напротив, соответствия для всех пакетов за исключением пакетов IPSec.

Форма **set** данной команды используется для указания типа пакетов, для которых будет установлено соответствие для указанного правила.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.87 filter-ipv6 <имя> rule <номер_правила> l7protocol <протокол>

Указание протокола для фильтрации пакетов на прикладном уровне.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> l7protocol <протокол>
delete filter-ipv6 <имя> rule <номер_правила> l7protocol <протокол>
show filter-ipv6 <имя> rule <номер_правила>  l7protocol
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      l7protocol протокол
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

протокол

Имя протокола прикладного уровня, используемого для фильтрации пакетов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для включения фильтрации сетевых пакетов на прикладном уровне. Для фильтрации на прикладном уровне используется механизм регулярных выражений, который позволяет определить тип используемого протокола.

При использовании фильтрации на прикладном уровне необходимо учитывать, что для корректной работы механизма классификатор трафика должен видеть весь имеющий значение для классификации трафик. Для этого под правило фильтрации трафика, в котором применяется фильтрация на прикладном уровне, должны подпадать все разновидности трафика, генерируемые классифицируемым протоколом. Так, например, если в таком правиле будет учитываться только трафик, идущий в одном направлении, но не будет учитываться трафик, идущий в рамках тех же соединений в обратную сторону, фильтрация в ряде случаев может выполняться некорректно.

Так как механизм фильтрации на прикладном уровне требует больших системных ресурсов по сравнению с фильтрацией на основе параметров источника и отправителя, рекомендуется в тех случаях, когда это возможно использовать механизм фильтрации на основе таких параметров получателя и отправителя, как номер используемого сетевого порта или IP-адрес.

Фильтрация на прикладном уровне может быть использована в тех случаях, когда:

- требуется установить соответствие для пакетов протоколов, использующих номера портов, которые не могут быть заранее предсказаны;
- требуется установить соответствие для пакетов протоколов при использовании нестандартных номеров портов (например, HTTP на порту 1111);
- требуется распознать протоколы, использующие одинаковые номера портов (например, обмен файлами P2P, использующий порт 80).

Фильтрация на прикладном уровне может быть использована для контроля полосы пропускания для указанных протоколов, для учета пакетов указанных протоколов или для блокировки пакетов. При использовании фильтрации на прикладном уровне для блокировки пакетов указанных протоколов без дополнительных мер следует помнить, что могут возникать как ошибочные срабатывания (один протокол похож на другой), так и ошибочные несрабатывания фильтров (приложения могут маскировать свой протокол обмена способами, не учитываемыми в фильтре).

Форма **set** данной команды позволяет указать протокол для фильтрации на прикладном уровне.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.88 filter-ipv6 <имя> rule <номер_правила> length

Указание параметров, ограничивающих длину пакетов для правила фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> length [layer <уровень> | value <длина>]
delete filter-ipv6 <имя> rule <номер_правила> length [layer | value]
show filter-ipv6 <имя> rule <номер_правила> length [layer | value]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
    rule номер_правила {
        length {
            layer уровень
            value длина
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

уровень

Уровень сетевой модели TCP/IP. Указать уровень согласно сетевой модели TCP/IP, на котором будет производиться проверка длины пакета. Допустимые значения приведены в таблице ниже.

Таблица 106 - Допустимые значения уровней сетевой модели TCP/IP

Значение	Описание
layer3	Сетевой уровень
layer4	Транспортный уровень
layer5	Прикладной уровень

длина

Длина пакета. Допустимые значения приведены в таблице ниже.

Таблица 107 - Допустимые значения длины пакета

Значение	Описание

Значение	Описание
<0-4294967295>	Соответствие для пакетов указанной длины
!<0-4294967295>	Соответствие для всех пакетов, за исключением имеющих указанную длину
<x-y>	Соответствие для пакетов указанного диапазона длин
!<x-y>	Соответствие для всех пакетов, кроме имеющих указанный диапазон длин

Значение по умолчанию

Ограничения не установлены.

Указания по использованию

Данная команда позволяет указать параметры, ограничивающие длину пакетов в правиле фильтрации трафика IPv6.

Форма **set** данной команды используется для указания параметров, ограничивающих длину пакетов в правиле фильтрации трафика.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.89 filter-ipv6 <имя> rule <номер_правила> limit connection-rate

Указание параметров, ограничивающих частоту прохождения пакетов для соединения в правиле фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила>limit connection-rate [above <макс_частота> | burst <размер> | destination-mask <маска_получателя> | group-by <режим> | source-mask <маска_источника> | upto <мин_частота>]

delete filter-ipv6 <имя> rule <номер_правила>limit connection-rate [above | burst | destination-mask | group-by | source-mask | upto]

show filter-ipv6 <имя> rule <номер_правила>limit connection-rate [above | burst | destination-mask | group-by | source-mask | upto]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
    rule номер_правила {
        limit {
            connection-rate {
                above макс_частота
                burst размер
                destination-mask маска_получателя
                group-by режим
                source-mask маска_источника
                upto мин_частота
            }
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

макс_частота

Максимальная частота прохождения сетевых пакетов, для которых было установлено соответствие критериям правила. Время может быть указано в следующих единицах: **second** (секунды), **minute** (минуты), **hour** (часы), а также **day** (дни). Допустимые значения для частоты прохождения сетевых пакетов приведены в таблице ниже.

Таблица 108 - Допустимые значения частоты прохождения сетевых пакетов

Значение	**Описание**
<1-10000>	Число пакетов в секунду
<1-10000>/second	Число пакетов в секунду
<1-600000>/minute	Число пакетов в минуту
<1-36000000>/hour	Число пакетов в час
<1-864000000>/day	Число пакетов за день

размер

Размер буфера групп пакетов. Задает число пакетов, которые могут быть переданы со скоростью, превышающей указанную. По умолчанию установлено значение равное 1, которое не допускает передачи групп пакетов со скоростью превышающей установленную. Значение должно находиться в диапазоне от 1 до 10000.

маска_получателя

Маска для группировки соединений по IP-адресу получателя. Значение должно находиться в диапазоне от 0 до 128.

режим

Режим группировки соединений. Допустимые значения для режима группировки соединений приведены в таблице ниже.

Таблица 109 - Допустимые значения режима группировки соединений

Значение	**Описание**
destination-address	Группировка по IPv6-адресу получателя
destination-port	Группировка по порту получателя
source-address	Группировка по IPv6-адресу отправителя
source-port	Группировка по порту отправителя

маска_источника

Маска для группировки соединений по IP-адресу отправителя. Значение должно находиться в диапазоне от 0 до 128.

мин_частота

Минимальная частота прохождения сетевых пакетов, для которых было установлено соответствие критериям правила. Ограничения на значения аналогичны значениям максимальной частоты.

Значение по умолчанию

Ограничение не установлено.

Указания по использованию

Данная команда позволяет указать параметры, ограничивающие частоту прохождения сетевых пакетов для соединения в правиле фильтрации трафика IPv6. При создании правила фильтрации, ограничивающего частоту прохождения сетевых пакетов для соединения, указание режима группировки соединений, а также максимальной или минимальной частоты является обязательным. Может быть указано либо максимальная, либо минимальная частота.

Форма **set** данной команды используется для указания параметров, ограничивающих частоту прохождения пакетов для соединения.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.90 filter-ipv6 <имя> rule <номер_правила> limit connections

Указание параметров, ограничивающих количество соединений в правиле фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила>limit connections [above <мин_кол-во> | group-by <режим> | mask <маска> | upto <макс_кол-во>]
delete filter-ipv6 <имя> rule <номер_правила>limit connections [above | mask]
show filter-ipv6 <имя> rule <номер_правила>limit connections [above | mask]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      limit {
         connections {
            above мин_кол-во
           group-by режим
           mask маска
           upto макс_кол-во
        }
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

мин_кол-во

Минимальное количество соединений. Значение должно находиться в диапазоне от 0 до 4294967295.

режим

Режим группировки соединений. Допустимые значения:

destination: Группировка по IPv6-адресу получателя;

source: Группировка по IPv6-адресу отправителя.

маска

Маска для группировки соединений по IP-адресу. Значение должно находиться в диапазоне от 0 до 128.

макс_кол-во

Максимальное количество соединений. Значение должно находиться в диапазоне от 0 до 4294967295.

Значение по умолчанию

Ограничение не установлено.

Указания по использованию

Данная команда позволяет указать параметры, ограничивающие количество соединений в правиле фильтрации трафика IPv6. При создании правила фильтрации, ограничивающего количество соединений, указание минимального или максимального числа соединений является обязательным. Может быть указано либо максимальное, либо минимальное количество соединений.

Форма **set** данной команды используется для указания параметров, ограничивающих количество соединений в правиле фильтрации трафика.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.91 filter-ipv6 <имя> rule <номер_правила> limit packet-rate

Указание параметров, ограничивающих частоту прохождения пакетов в правиле фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> limit packet-rate [burst <размер> | rate <частота>]

delete filter-ipv6 <имя> rule <номер_правила> limit packet-rate [burst | rate]

show filter-ipv6 <имя> rule <номер_правила> limit packet-rate [burst | rate]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
    rule номер_правила {
        limit {
            packet-rate {
                burst размер
                rate частота
            }
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

размер

Размер буфера групп пакетов. Максимальное число пакетов, которые могут быть переданы со скоростью, превышающей указанную. По умолчанию установлено значение равное 1, которое не допускает передачи групп пакетов со скоростью превышающей установленную. Значение должно находиться в диапазоне от 1 до 10000.

частота

Частота прохождения сетевых пакетов, для которых было установлено соответствие критериям правила. Время может быть указано в следующих единицах: **second** (секунды), **minute** (минуты), **hour** (часы), а также **day** (дни). Допустимые значения для частоты прохождения сетевых пакетов приведены в таблице ниже.

Таблица 110 - Допустимые значения частоты прохождения сетевых пакетов

Значение	**Описание**
<1-10000>	Число пакетов в секунду
<1-10000>/second	Число пакетов в секунду
<1-600000>/minute	Число пакетов в минуту
<1-36000000>/hour	Число пакетов в час
<1-864000000>/day	Число пакетов за день

Значение по умолчанию

Ограничение не установлено.

Указания по использованию

Данная команда используется для ограничения частоты прохождения сетевых пакетов, для которых установлено соответствие данному правилу. Для ограничения частоты прохождения входящих сетевых пакетов используется фильтр TBF (Token Bucket Filter), который позволяет административно задать требуемую пропускную способность, а также возможность ее превышения для коротких групп пакетов.

Для реализации TBF используется буфер (bucket), который постоянно заполняется маркерами (token) с установленной скоростью (token rate). Наиболее важным параметром буфера является его размер, то есть число маркеров, которое в нем может содержаться. Каждый прибывающий маркер сопоставляется с одним пакетом данных из очереди данных, после чего удаляется из буфера. При работе данного алгоритма возможны три различных варианта:

Данные прибывают со скоростью **равной** скорости входящих маркеров. В этом случае каждый пакет имеет соответствующий маркер и проходит очередь без задержки.

Данные прибывают со скоростью **меньшей** скорости поступления маркеров. В этом случае лишь часть существующих маркеров будет уничтожаться, таким образом, они станут накапливаться до размера буфера. Накопленные маркеры могут использоваться для передачи групп пакетов со скоростью, превышающей установленную скорость прибывающих маркеров.

Данные прибывают **быстрее**, чем маркеры. Это означает, что в определенный момент в буфере не останется маркеров, что заставит алгоритм приостановить передачу данных. Эта ситуация называется "превышением". Если пакеты продолжают поступать, они начинают уничтожаться.

Форма **set** данной команды используется для указания параметров, ограничивающих частоту прохождения пакетов.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.92 filter-ipv6 <имя> rule <номер_правила> log <состояние>

Включение или отключение регистрации для действий правила фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> log <состояние>
delete filter-ipv6 <имя> rule <номер_правила> log <состояние>
show filter-ipv6 <имя> rule <номер_правила> log
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      log состояние
```

```
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

состояние

Включение или отключение регистрации действий фильтра трафика. Допустимые значения:

enable: Включить регистрацию действий;

disable: Отключить регистрацию действий.

Значение по умолчанию

Регистрация действий отключена.

Указания по использованию

Данная команда используется для включения или отключения регистрации действия для указанного правила.

ПРИМЕЧАНИЕ Регистрация действия происходит только используемого фильтра, т.е такого фильтра, который применен к какой-либо политике. Эта политика, в свою очередь, должна быть применена к какому-либо направлению трафика. В противном случае фильтр считается настроенным, но не активным.

Сообщения регистрации для правил фильтрации трафика записываются в журнал регистрации от имени программы **kernel** с уровнем серьезности **warning**. При регистрации пакета в журнале регистрации указывается имя фильтра и его номер.

Например, для сетевого пакета который попадает под правило 10 фильтра трафика с именем **test**, в журнал регистрации будет помещена запись **[test-10]**. Если правило фильтра трафика было правилом исключения (атрибут **exclude**), то в журнал регистрации будет помещена запись **[test-10-E]**.

Форма **set** данной команды позволяет включить регистрацию указанного правила.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.93 filter-ipv6 <имя> rule <номер_правила> p2p <имя_приложения>

Указание одноранговогo приложения для фильтрации его IPv6-пакетов на прикладном уровне.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> p2p <имя_приложения>
delete filter-ipv6 <имя> rule <номер_правила> p2p <имя_приложения>
show filter-ipv6 <имя> rule <номер_правила> p2p
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      p2p {
         имя_приложения
     }
```

```
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

имя_приложения

Обязательный. Соответствие устанавливается для пакетов одноранговового приложения. Допустимые значения приведены в таблице ниже.

Таблица 111 - Допустимые значения одноранговых приложений

Значение	Описание
all	Соответствие устанавливается для пакетов любого из приложений, перечисленных в данной таблице
applejuice	Соответствие устанавливается для пакетов приложения AppleJuice
bittorrent	Соответствие устанавливается для пакетов приложения BitTorrent
directconnect	Соответствие устанавливается для пакетов приложения Direct Connect
edonkey	Соответствие устанавливается для пакетов приложения eDonkey/eMule
gnutella	Соответствие устанавливается для пакетов приложения Gnutella
kazaa	Соответствие устанавливается для пакетов приложения KaZaA

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания одноранговового приложения, пакеты которого будут фильтроваться. Фильтрация происходит на прикладном уровне. Для пакетов, отправленных указанным приложением или предназначенных для него, будет установлено соответствие критериям данного правила. В правиле может быть указано несколько одноранговых приложений.

Форма **set** данной команды используется для указания одноранговового приложения, к пакетам которого будет применяться правило.

Форма **delete** данной команды используется для удаления настройки одноранговового приложения для указанного правила.

Форма **show** данной команды используется для отображения настройки.

16.2.94 filter-ipv6 <имя> rule <номер_правила> probability <вероятность>

Указание вероятности срабатывания правила в процентах.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> probability <вероятность>
delete filter-ipv6 <имя> rule <номер_правила> probability
show filter-ipv6 <имя> rule <номер_правила> probability
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
    rule номер_правила {
        probability вероятность
```

```
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

вероятность

Вероятность срабатывания правила в процентах. Обязательный параметр. Значение должно находиться в диапазоне от 1 до 99.

Значение по умолчанию

Не установлено.

Указания по использованию

Данная команда используется для указания вероятности срабатывания правила в процентах от 1 до 99.

Форма **set** данной команды используется для указания вероятности срабатывания правила.

Форма **delete** данной команды используется для удаления установленного значения.

Форма **show** данной команды используется для отображения установленного значения для вероятности срабатывания правила.

16.2.95 filter-ipv6 <имя> rule <номер_правила> protocol <протокол>

Указание протокола для фильтрации пакетов.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> protocol <протокол>
delete filter-ipv6 <имя> rule <номер_правила> protocol <протокол>
show filter-ipv6 <имя> rule <номер_правила> protocol
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
    rule номер_правила {
        protocol протокол
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

протокол

Обязательный. Могут быть использованы любые наименования протоколов или их номера, определенные в файле /etc/protocols. Допустимые значения приведены в таблице ниже.

Таблица 112 - Допустимые значения для указания протокола

Значение	Описание

all	Соответствие устанавливается для всех протоколов IPv6
tcp_udp	Соответствие устанавливается для протоколов TCP и UDP
<0-255>	Соответствие устанавливается для указанного номера протокола IPv6
<text>	Соответствие устанавливается для указанного имени протокола IPv6
!<0-255>	Соответствие устанавливается для всех протоколов IPv6, кроме указанного
!<text>	Соответствие устанавливается для всех протоколов IPv6, кроме указанного

Значение по умолчанию

По умолчанию определены все протоколы.

Указания по использованию

Данная команда используется для определения критерия соответствия на основе указанного протокола. Для пакетов указанного протокола будет установлено соответствие данному правилу.

Следует с осторожностью включать в набор правил более одного правила, определяющего исключения (правило, в котором указывается восклицательный знак "!"). Правила фильтра трафика выполняются по порядку, при этом последовательность правил, определяющих исключения, может привести к непредсказуемым результатам.

Форма **set** данной команды используется для указания протокола, к пакетам которого будет применяться указанное правило.

Форма **delete** данной команды используется для удаления установленного значения.

Форма **show** данной команды используется для отображения установленного значения.

16.2.96 filter-ipv6 <имя> rule <номер_правила> quota overall

Настройка квотирования фильтрации пакетов по всему объёму данных или числу пакетов.

Синтаксис

```
set filter-ipv6 <имя>  rule <номер_правила> quota overall [invert | mode <режим_квотирования> | upto <макс_число>]

delete filter-ipv6 <имя>  rule <номер_правила> quota overall [invert | mode | upto]

show filter-ipv6 <имя>  rule <номер_правила> quota overall [invert | mode | upto]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
    rule номер_правила {
        quota {
            overall {
                invert
                mode режим_квотирования
                upto макс_число
            }
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

invert

Необязательное ключевое слово. Если оно не указано, то правило будет срабатывать до тех пор, пока заданное значение счётчика не будет превышено. Если ключевое слово **invert** указано, то поведение будет обратным: правило не будет срабатывать, пока заданное значение не будет превышено.

режим_квотирования

Определяет один из двух режимов квотирования:

bytes: Квотирование по объёму данных;

packets: Квотирование по числу пакетов.

макс_число

Определяет максимальный объём данных или число пакетов. Объём данных может быть указан в следующих единицах: kb (килобайты), mb (мегабайты), gb (гигабайты). Допустимые значения приведены в таблице ниже.

Таблица 113 - Допустимые значения для указания максимального объёма данных или числа пакетов

Значение	Описание
<1-18446744073709551615>	Максимальное количество пакетов, если указан режим packets (2^64 -1)
<1-18446744073709551615>	Максимальный объём данных (в байтах), если указан режим bytes (2^64 -1)
<1-18014398509481983>kb	Максимальный объём данных (в килобайтах), только для режима bytes (2^54 -1)
<1-17592186044415>mb	Максимальный объём данных (в мегабайтах), только для режима bytes (2^44 -1)
<1-17179869183>gb	Максимальный объём данных (в гигабайтах), только для режима bytes (2^34 -1)

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать режим квотирования и объём квоты пакетов для правила фильтрации трафика IPv6 без учёта направления движения пакетов.

Форма **set** данной команды используется для указания режима квотирования и объёма квоты пакетов для правила фильтрации трафика.

Форма **delete** данной команды используется для удаления установленного значения.

Форма **show** данной команды используется для отображения установленного значения.

16.2.97 filter-ipv6 <имя> rule <номер_правила> quota per-connection

Настройка квотирования фильтрации пакетов по объёму данных или числу пакетов на соединение.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> quota per-connection [count-direction <направление_движения> | mode <режим_квотирования >| upto <макс_число>]

delete filter-ipv6 <имя> rule <номер_правила> quota per-connection [count-direction | mode | upto]

show filter-ipv6 <имя> rule <номер_правила> quota per-connection [count-direction | mode | upto]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
```

```
    rule номер_правила {
       quota {
          per-connection {
             count-direction направление_движения
             mode режим_квотирования
             upto макс_число
          }
       }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

направление_движения

Необязательный. Направление движения пакетов, которое стоит учитывать. Допустимые значения для направления движения пакетов приведены в таблице ниже.

Таблица 114 - Допустимые значения для направления движения пакетов

Значение	**Описание**
original	Учитываются пакеты от инициатора соединения
reply	Учитываются пакеты к инициатору соединения
both	Учитываются пакеты для обоих направлений

По умолчанию учитываются пакеты для обоих направлений.

режим_квотирования

Определяет один из двух режимов квотирования:

bytes: Квотирование по объёму данных;

packets: Квотирование по числу пакетов.

макс_число

Определяет максимальный объём данных или число пакетов. Объём данных может быть указан в следующих единицах: kb (килобайты), mb (мегабайты), gb (гигабайты). Допустимые значения приведены в таблице ниже.

Таблица 115 - Допустимые значения для указания максимального объёма данных или числа пакетов

Значение	**Описание**
<1-4294967295>	Максимальное количество пакетов, если указан режим packets (2^32 -1)
<1-4294967295>	Максимальный объём данных (в байтах), если указан режим bytes (2^32 -1)
<1-4194303>kb	Максимальный объём данных (в килобайтах), только для режима bytes (2^22 -1)
<1-4095>mb	Максимальный объём данных (в мегабайтах), только для режима bytes (2^12 -1)
<1-3>gb	Максимальный объём данных (в гигабайтах), только для режима bytes (2^2 -1)

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать режим квотирования и объём квоты пакетов для правила фильтрации трафика IPv6 с учётом направления движения пакетов.

Форма **set** данной команды используется для указания режима квотирования и объёма квоты пакетов для правила фильтрации трафика.

Форма **delete** данной команды используется для удаления установленного значения.

Форма **show** данной команды используется для отображения установленного значения.

16.2.98 filter-ipv6 <имя> rule <номер_правила> recent

Установка соответствия для сетевых пакетов от недавно встречавшихся отправителей.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> recent [count <счетчик> | time <секунды>]
delete filter-ipv6 <имя> rule <номер_правила> recent [count | time]
show filter-ipv6 <имя> rule <номер_правила> recent [count | time]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
     recent {
         count счетчик
         time секунды
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

счетчик

Обязательный. Количество пакетов с одинаковым IP-адресом отправителя, необходимое для срабатывания правила. Значение должно находиться в диапазоне от 1 до 20.

секунды

Обязательный. Количество времени, указываемое в секундах, в течение которого будет происходить подсчет пакетов от одного отправителя. Значение должно находиться в диапазоне от 1 до 4294967295.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет установить соответствие для сетевых пакетов, пришедших от недавно встречавшихся отправителей.

Форма **set** данной команды позволяет установить настройку для проверки соответствия на основе адресов недавно встречавшихся отправителей.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.99 filter-ipv6 <имя> rule <номер_правила> sctp chunk-type

Установка параметров протокола SCTP для проверки соответствия в правиле фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя>rule <номер_правила> sctp chunk-type [invert | logic <режим_сопоставления>| type <тип>]
delete filter-ipv6 <имя>rule <номер_правила> sctp chunk-type [invert | logic | type <тип>]
show filter-ipv6 <имя>rule <номер_правила> sctp chunk-type [logic | type]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      sctp {
         chunk-type {
            invert
            logic режим_сопоставления
            type {
               тип
            }
         }
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

invert

Необязательное ключевое слово. Если оно указано то производится инверсия сопоставления.

режим_сопоставления

Обязательный. Логика обработки пакетов с указанными типами блоков. Допустимые значения приведены в таблице ниже.

Таблица 116 - Допустимые значения для режима сопоставления пакетов с указанными типами блоков

Значение	Описание
any	Соответствие устанавливается при совпадении любого из указанных типов
All	Соответствие устанавливается при совпадении всех указанных типов
only	Соответствие устанавливается при совпадении всех указанных типов и отсутствию иных типов

По умолчанию используется режим сопоставления **any**.

тип

Обязательный. Тип блока для сопоставления. Допустимые значения типов блоков приведены в таблице ниже.

Таблица 117 - Допустимые значения для указания типов блоков

Значение	**Описание**
abort	Разрыв ассоциации (ABORT, код 6)
asconf	Смена адресной настройки (ASCONF, код 193)
asconf-ack	Подтверждение адресной конфигурации (ASCONF ACK, код 128)
cookie-ack	Подтверждение маркера (COOKIE ACK, код 11)
cookie-echo	Маркерное отражение (COOKIE ECHO, код 10)
data	Данные (DATA, код 0)
ecn-cwr	Окно перегрузки уменьшено (CWR, код 13)
ecn-ecne	Отражение явного уведомления о перегруженности (ECN ECHO, код 12)
error	Ошибка взаимодействия (ERROR, код 9)
forward-tsn	Смещение накопленного порядкового номера передачи (FORWARD TSN, код 192)
heartbeat	Запрос состояния соединения (HEARTBEAT, код 4)
heartbeat-ack	Подтверждение запроса проверки состояния соединения (HEARTBEAT ACK, код 5)
init	Инициализация (INIT, код 1)
init-ack	Подтверждение инициализации (INIT ACK, код 2)
sack	Частичное подтверждение (SACK, код 3)
shutdown	Закрытие ассоциации (SHUTDOWN, код 7)
shutdown-ack	Подтверждение закрытия ассоциации (SHUTDOWN ACK, код 8)
shutdown-complete	Окончание закрытия ассоциации (SHUTDOWN COMPLETE, код 14)

Одновременно можно задать более одно типа блоков.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать параметры протокола SCTP для проверки соответствия правилу фильтрации.

Предварительно должен быть определен протокол SCTP при помощи команды *filter-ipv6 <имя> rule <номер_правила> protocol sctp*.

Форма **set** используется для включения фильтрации по протоколу SCTP и указания параметров.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.100 filter-ipv6 <имя> rule <номер_правила> source address <адрес>

Указание адреса отправителя для проверки соответствия в правиле фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> source address <адрес>
delete filter-ipv6 <имя> rule <номер_правила> source address <адрес>
show filter-ipv6 <имя> rule <номер_правила> source address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      source {
         address адрес
```

```
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

адрес

Адрес отправителя, используемый для проверки соответствия. Поддерживаемые значения приведены в таблице ниже.

Таблица 118 - Поддерживаемые значения адреса отправителя

Значение	Описание
<h:h:h:h:h:h:h:h>	Адрес IPv6
<h:h:h:h:h:h:h:h/x>	Подсеть IPv6 (значение ::/0 соответствует любой сети)
<h:h:h:h:h:h:h:h>-<h:h:h:h:h:h:h:h>	Диапазон IPv6-адресов
!<h:h:h:h:h:h:h:h>	Соответствие будет установлено для всех IPv6-адресов, кроме указанного
!<h:h:h:h:h:h:h:h/x>	Соответствие будет установлено для всех IPv6-адресов, кроме указанной подсети
!<h:h:h:h:h:h:h:h>-<h:h:h:h:h:h:h:h>	Соответствие будет установлено для всех IPv6-адресов, кроме адресов, входящих в указанный диапазон

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать адрес отправителя в правиле фильтрации трафика IPv6.

В том случае если явно указаны адрес и номер порта, для пакета устанавливается соответствие критериям правила в том и только том случае, если совпадает как адрес, так и номер порта.

Форма **set** данной команды используется для указания адреса отправителя в правиле фильтрации трафика.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.101 filter-ipv6 <имя> rule <номер_правила> source address-type <тип>

Указание типа адреса отправителя, по которому будет осуществляться проверка соответствия в правиле фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> source address-type <тип>
delete filter-ipv6 <имя> rule <номер_правила> source address-type <тип>
show filter-ipv6 <имя> rule <номер_правила> source address-type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
    rule номер_правила {
        source {
```

```
            address-type тип
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

тип

Тип адреса отправителя (источника). Данное правило будет применено к пакетам, тип адреса отправителя (источника) которых соответствует указанному. Допустимые значения приведены в таблице ниже.

Таблица 119 - Допустимые значения типа адреса отправителя

Значение	Описание
unspec	Неопределённый адрес (::)
unicast	Однонаправленный адрес
local	Локальный адрес
multicast	Мультивещательный адрес
anycast	Близковещательный адрес (anycast)
unreachable	Недостижимый адрес

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать тип адреса отправителя в правиле фильтрации трафика IPv6.

Форма **set** данной команды используется для создания настройки типа адреса источника для правила фильтрации трафика.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.102 filter-ipv6 <имя> rule <номер_правила> source country <код_страны>

Указание двухзначного кода страны отправителя в правиле фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> source country <код_страны>
delete filter-ipv6 <имя> rule <номер_правила> source country <код_страны>
show filter-ipv6 <имя> rule <номер_правила> source country
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
    rule номер_правила {
        source {
            country код_страны
        }
```

```
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

код_страны

Двузначный код страны отправителя.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания двухзначного кода страны отправителя в правиле фильтрации трафика IPv6. В одном правиле фильтрации может быть задано не более 16 стран.

ПРИМЕЧАНИЕ Необходимо иметь в виду, что данные о принадлежности IP диапазона к определенному региону берутся из общедоступных источников и могут не обладать 100% точностью. Для дополнения/исключения диапазонов рекомендуется использовать группы IP адресов (groups address-group) в правилах фильтрации.

Форма **set** данной команды используется для указания двухзначного кода страны источника в правиле фильтрации трафика IPv6.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для просмотра настройки.

16.2.103 filter-ipv6 <имя> rule <номер_правила> source local-group <имя_группы>

Указание локальной группы МЭ для проверки соответствия в правиле фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> source local-group <имя_группы>
delete filter-ipv6 <имя> rule <номер_правила> source local-group <имя_группы>
show filter-ipv6 <имя> rule <номер_правила> source local-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      source {
         local-group имя_группы
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

имя_группы

Имя локальной группы МЭ. Допустимые значения представлены в таблице ниже.

Таблица 120 - Допустимые значения для локальной группы

Значение	Описание
<text>	Имя группы
!<text>	Все группы кроме указанной

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать локальную группу МЭ для сопоставления в правиле фильтрации трафика IPv6.

Форма **set** данной команды используется для указания локальной группы МЭ в правиле фильтрации трафика IPv6.

Форма **delete** данной команды используется для удаления локальной группы МЭ в правиле фильтрации трафика IPv6.

Форма **show** данной команды используется для отображения настройки локальной группы МЭ в правиле фильтрации трафика IPv6.

ПРИМЕЧАНИЕ При использовании политикой фильтра с заданными локальными пользователями/группами, такая политика может быть использована только в качестве системной.

16.2.104 filter-ipv6 <имя> rule <номер_правила> source local-user <имя_пользователя>

Указание локального пользователя МЭ для проверки соответствия в правиле фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> source local-user <имя_пользователя>
delete filter-ipv6 <имя> rule <номер_правила> source local-user <имя_пользователя>
show filter-ipv6 <имя> rule <номер_правила> source local-user
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      source {
         local-user имя_пользователя
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

имя_пользователя

Имя локального пользователя МЭ. Допустимые значения представлены в таблице ниже.

Таблица 121 - Допустимые значения для локального пользователя

Значение	Описание
<text>	Имя пользователя
!<text>	Все пользователи кроме указанного

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать локального пользователя МЭ для сопоставления в правиле фильтрации трафика IPv6.

Форма **set** данной команды используется для указания локального пользователя МЭ в правиле фильтрации трафика IPv6.

Форма **delete** данной команды используется для удаления локального пользователя МЭ в правиле фильтрации трафика IPv6.

Форма **show** данной команды используется для отображения настройки локального пользователя МЭ в правиле фильтрации трафика IPv6.

ПРИМЕЧАНИЕ При использовании политикой фильтра с заданными локальными пользователями/группами, такая политика может быть использована только в качестве системной.

16.2.105 filter-ipv6 <имя> rule <номер_правила> source mac-address <mac-адрес>

Указание MAC-адреса отправителя, по которому будет осуществляться проверка соответствия в правиле фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> source mac-address <mac-адрес>
delete filter-ipv6 <имя> rule <номер_правила> source mac-address <mac-адрес>
show filter-ipv6 <имя> rule <номер_правила> source mac-address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      source {
         mac-address mac-адрес
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

mac-адрес

MAC-адрес для проверки соответствия. Адрес указывается в формате шести разделенных двоеточиями 8-битных шестнадцатеричных чисел, например 00:0a:59:9a:f2:ba.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать MAC-адрес источника, по которому будет осуществляться проверка соответствия пакета критериям правила фильтрации трафика.

Форма **set** данной команды используется для указания MAC-адреса отправителя в правиле фильтрации трафика.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.106 filter-ipv6 <имя> rule <номер_правила> source port <порт>

Указание номера сетевого порта отправителя для проверки соответствия в правиле фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя>rule  <номер_правила> source port <порт>
delete filter-ipv6 <имя>rule <номер_правила> source port <порт>
show filter-ipv6 <имя>rule <номер_правила> source port
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      source {
         port порт
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

порт

Порт отправителя для проверки соответствия. Допустимые значения представлены в таблице ниже:

Таблица 122 – Формат указания порта получателя

Значение	Описание
<text>	Имя порта (любое из файла /etc/services)
<0-65535>	Номер порта
<start>-<end>	Диапазон портов

Возможно также задание списка через запятую, например: "22,telnet,http,123,1001-1005".

Возможно также задание инвертированного списка с помощью "!", например: "!22,telnet,http,123,1001-1005".

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать номера сетевого порта отправителя в правиле фильтрации трафика IPv6. Сетевой порт может быть указан только для протоколов TCP, UDP, SCTP и DCCP. Предварительно должен быть определен протокол при помощи команды *filter-ipv6 <имя> rule <номер_правила> protocol <протокол>*.

В том случае если явно указаны адрес и номер порта, для пакета устанавливается соответствие критериям правила в том и только том случае, если совпадает как адрес, так и номер порта.

Форма **set** данной команды используется для указания порта отправителя в правила фильтрации трафика IPv6.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

16.2.107 filter-ipv6 <имя> rule <номер_правила> state

Указание состояний соединений, к которым применяется правило фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> state [established <состояние> | invalid <состояние> | new <состояние> | related <состояние>]

delete filter-ipv6 <имя> rule <номер_правила> state [established | invalid | new | related]

show filter-ipv6 <имя> rule <номер_правила> state
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
    rule номер_правила {
        state {
            established состояние
            invalid состояние
            new состояние
            related состояние
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

established *состояние*

Позволяет указать, следует ли применять данное правило к пакетам установленных соединений. Поддерживаются следующие значения:

enable: Применить правило к пакетам установленных соединений;

disable: Не применять правило к пакетам установленных соединений.

invalid *состояние*

Позволяет указать, следует ли применять данное правило к пакетам недействительных соединений. Поддерживаются следующие значения:

enable: Применить правило к пакетам недействительных соединений;

disable: Не применять правила к пакетам недействительных соединений.

new *состояние*

Позволяет указать, следует ли применять данное правило к пакетам новых соединений. Поддерживаются следующие значения:

enable: Применить правило к пакетам новых соединений;

disable: Не применять правило к пакетам новых соединений.

related *состояние*

Позволяет указать, следует ли применять данное правило к пакетам связанных соединений. Поддерживаются следующие значения:

enable: Применить данное правило к пакетам связанных соединений;

disable: Не применять данное правило к пакетам связанных соединений.

Значение по умолчанию

Указанное правило применяется ко всем пакетам вне зависимости от состояния соединения.

Указания по использованию

Данная команда позволяет указать состояния соединений, к пакетам которых будет применяться данное правило фильтрации трафика IPv6.

Established - состояние установленного соединения. Соединение считается установленным в том случае, когда был получен трафик в обоих направлениях.

Invalid - состояние недействительного соединения. Присваивается пакетам, которые не могут быть идентифицированы по каким-либо причинам. Такое возможно в случае нехватки ресурсов системы для обработки пакета; или если пакет не содержит сведений идентифицирующих состояние; или ошибки ICMP, которые не могут быт соотнесены ни с одним известным соединением. Обычно эти пакеты отбрасываются.

New - состояние нового соединения. Такое состояние характерно для пакетов, впервые встреченных системой, содержащих информацию о новом соединении. Для протокола TCP, это пакеты с установленным флагом SYN.

Related - состояние связанного соединения. Такое состояние характерно для соединений, инициированных на основе уже существующего установленного соединения. В качестве примера можно привести соединение для обмена данными протокола FTP, которое будет являться связанным по отношению к установленному управляющему соединению FTP.

Форма **set** данной команды позволяет указать тип пакетов, к которому будет применяться правило фильтрации трафика IPv6.

Форма **delete** данной команды позволяет восстановить поведение, принятое по умолчанию.

Форма **show** данной команды используется для отображения настройки.

ПРИМЕЧАНИЕ При использовании в конфигурации данного фильтра на устройстве производится дефрагментация пакетов. В случае дефрагментации пакетов фильтр фрагментации fragment не будет отрабатывать.

16.2.108 filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> case-insensitive

Не учитывать регистр букв при фильтрации по подстрокам в IPv6-пакете.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> case-insensitive

delete filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> case-insensitive

show filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> case-insensitive
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      string номер_подстроки {
         case-insensitive
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

номер_подстроки

Множественный узел. Численный идентификатор подстроки. Для установки соответствия на основе нескольких подстрок, следует создать соответствующее количество узлов **string** в одном правиле фильтра трафика, в этом случае соответствие будет установлено только для пакетов, в которых будут обнаружены все указанные подстроки.

case-insensitive

При указании данного параметра поиск будет осуществляться без учета регистра букв в подстроке.

Значение по умолчанию

По умолчанию регистр букв учитывается.

Указания по использованию

При использовании этой команды при поиске подстроки в пакете IPv6 не учитывается регистр букв. Предварительно должна быть определена искомая подстрока при помощи команды *filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> match <подстрока>* или в шестнадцатеричной нотации при помощи команды *filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> hex-match <подстрока>*.

Форма **set** данной команды позволяет указать, что требуется не учитывать регистр букв при поиске подстроки.

Форма **delete** данной команды позволяет восстановить поведение, принятое по умолчанию.

Форма **show** данной команды используется для отображения настройки.

16.2.109 filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> from <смещение>

Установка смещения в пакете IPv6, начиная с которого будет осуществляться поиск подстроки.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> from <смещение>
delete filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> from
show filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> from
```

Режим интерфейсач

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      string номер_подстроки {
         from смещение
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

номер_подстроки

Множественный узел. Численный идентификатор подстроки. Для установки соответствия на основе нескольких подстрок, следует создать соответствующее количество узлов **string** в одном правиле фильтра трафика, в этом случае соответствие будет установлено только для пакетов, в которых будут обнаружены все указанные подстроки.

смещение

Смещение в байтах от начала пакета IPv6. Значение должно находиться в диапазоне от 0 до 65535.

Значение по умолчанию

По умолчанию установлено значение 0, поиск подстроки осуществляется от начала пакета IPv6.

Указания по использованию

Данная команда позволяет указать смещение в пакете IPv6, начиная от которого, будет осуществляться поиск подстроки. Предварительно должна быть определена искомая подстрока при помощи команды *filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> match <подстрока>* или в шестнадцатеричной нотации при помощи команды *filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> hex-match <подстрока>*.

Смещение, до которого осуществляется поиск, указывается при помощи команды *filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> to <смещение>*.

Форма **set** данной команды позволяет указать смещение в пакете IPv6, начиная с которого будет осуществляться поиск подстроки в пакете IPv6.

Форма **delete** данной команды позволяет удалить настройку и восстановить значение, принятое по умолчанию.

Форма **show** данной команды используется для отображения настройки.

16.2.110 filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> hex-match <подстрока>

Указание подстроки для поиска в шестнадцатеричном виде.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> hex-match <подстрока>

delete filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> hex-match <подстрока>

show filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> hex-match
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      string номер_подстроки {
         hex-match подстрока
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

номер_подстроки

Множественный узел. Численный идентификатор подстроки. Для установки соответствия на основе нескольких подстрок, следует создать соответствующее количество узлов **string** в одном правиле фильтра трафика, в этом случае соответствие будет установлено только для пакетов, в которых будут обнаружены все указанные подстроки.

подстрока

Подстрока для поиска в пакете IPv6. Значение указывается в следующем формате: *текст|xx xx|текст*, где шестнадцатеричное значение ограничено символом ' | ', а шестнадцатеричные блоки (xx), представляющие байт данных, могут быть разделены пробелами, например, |40 41 42 43|. Значение *текст|xx xx|текст* необходимо заключить либо в одинарные (*'текст|xx xx|текст'*), либо в двойные (*"текст|xx xx|текст"*) кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет задать критерий соответствия для пакетов на основе подстроки для поиска в пакете IPv6, значение которой указывается в шестнадцатеричном виде.

Форма **set** данной команды позволяет указать значение подстроки для поиска в шестнадцатеричном виде.

Форма **delete** данной команды позволяет удалить настройку.

Форма **show** данной команды используется для отображения настройки.

16.2.111 filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> match <подстрока>

Указание подстроки для поиска.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> match <подстрока>

delete filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> match <подстрока>

show filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> match
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
  rule номер_правила {
     string номер_подстроки {
        match подстрока
     }
  }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

номер_подстроки

Множественный узел. Численный идентификатор подстроки. Для установки соответствия на основе нескольких подстрок, следует создать соответствующее количество узлов **string** в одном правиле фильтра трафика, в этом случае соответствие будет установлено только для пакетов, в которых будут обнаружены все указанные подстроки.

подстрока

Подстрока для поиска в пакете IPv6.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет задать критерий соответствия для пакетов на основе подстроки для поиска в пакете IPv6. Для того чтобы осуществлять поиск на основе нескольких подстрок, следует для одного правила фильтра трафика указать несколько узлов конфигурации **string**, в этом случае соответствие будет установлено только для пакетов, в которых будут обнаружены все указанные подстроки.

Форма **set** данной команды позволяет указать значение подстроки для поиска.

Форма **delete** данной команды позволяет удалить настройку.

Форма **show** данной команды используется для отображения настройки.

16.2.112 filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> negation

Установка соответствия на основе отсутствия указанной подстроки в пакете IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> negation

delete filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> negation
```

```
show filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> negation
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
   rule номер_правила {
      string номер_подстроки {
         negation
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

номер_подстроки

Множественный узел. Численный идентификатор подстроки. Для установки соответствия на основе нескольких подстрок, следует создать соответствующее количество узлов **string** в одном правиле фильтра трафика, в этом случае соответствие будет установлено только для пакетов, в которых будут обнаружены все указанные подстроки.

Значение по умолчанию

Отсутствует.

Указания по использованию

При указании команды соответствие будет устанавливаться для пакетов, в которых отсутствует указанная подстрока. Предварительно должна быть определена искомая подстрока при помощи команды *filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> match <подстрока>* или в шестнадцатеричной нотации при помощи команды *filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> hex-match <подстрока>*.

Форма **set** данной команды позволяет указать, что соответствие будет устанавливаться для пакетов, в которых отсутствует указанная подстрока.

Форма **delete** данной команды позволяет удалить настройку.

Форма **show** данной команды используется для отображения настройки.

16.2.113 filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> to <смещение>

Установка смещения в пакете IPv6, до которого будет осуществляться поиск подстроки.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> to
<смещение>
delete filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> to
show filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> to
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
```

```
    rule номер_правила {
        string номер_подстроки {
            to смещение
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

номер_подстроки

Множественный узел. Численный идентификатор подстроки. Для установки соответствия на основе нескольких подстрок, следует создать соответствующее количество узлов **string** в одном правиле фильтра трафика, в этом случае соответствие будет установлено только для пакетов, в которых будут обнаружены все указанные подстроки.

смещение

Смещение в байтах от начала пакета IPv6. Значение должно находиться в диапазоне от 0 до 65535.

Значение по умолчанию

По умолчанию поиск подстроки осуществляется до конца пакета IPv6.

Указания по использованию

Данная команда позволяет указать смещение в пакете IPv6, до которого, будет осуществляться поиск подстроки. Предварительно должна быть определена искомая подстрока при помощи команды *filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> match <подстрока>* или в шестнадцатеричной нотации при помощи команды *filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> hex-match <подстрока>*.

Смещение, от которого начинается поиск, указывается при помощи команды *filter-ipv6 <имя> rule <номер_правила> string <номер_подстроки> from <смещение>*.

Форма **set** данной команды позволяет указать смещение в пакете IPv6, до которого будет осуществляться поиск подстроки в пакете IPv6.

Форма **delete** данной команды позволяет удалить настройку и восстановить значение, принятое по умолчанию.

Форма **show** данной команды используется для отображения настройки.

16.2.114 filter-ipv6 <имя> rule <номер_правила> tcp flags <флаг>

Указание флагов TCP для проверки соответствия в правиле фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила>  tcp flags <флаг>
delete filter-ipv6 <имя> rule <номер_правила>  tcp flags
show filter-ipv6 <имя> rule <номер_правила> tcp flags
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
    rule номер_правила {
        tcp {
```

```
            flags флаг
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

флаг

Указание флагов TCP для проверки соответствия. Поддерживаются следующие значения: SYN, ACK, FIN, RST, URG, PSH и ALL. При указании нескольких флагов, они должны быть указаны через запятую. Например, при указании "SYN, !ACK, !FIN, !RST" будет установлено соответствие только в том случае, если установлен флаг SYN и не установлены флаги ACK, FIN, RST. Указание ALL может быть использовано для проверки того, что установлены все флаги, указание !ALL используется для проверки того, что не установлено ни одного флага. При указании перед значением флага восклицательного знака ("!") соответствие будет установлено в том случае, если флаг не установлен.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет проверять соответствие сетевых пакетов критериям правила фильтрации трафика IPv6 на основе флагов TCP. Предварительно должен быть определен протокол TCP для правила фильтрации при помощи команды *filter-ipv6 <имя> rule <номер_правила> protocol tcp*.

Форма **set** данной команды используется для указания флагов TCP на основе которых будет осуществляться проверка соответствия.

Форма **delete** данной команды позволяет восстановить поведение по умолчанию.

Форма **show** данной команды позволяет отобразить настройку.

16.2.115 filter-ipv6 <имя> rule <номер_правила> tcp mss <значение>

Указание максимального размера сегмента для проверки соответствия в правиле фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> tcp mss <значение>
delete filter-ipv6 <имя> rule <номер_правила> tcp mss
show filter-ipv6 <имя> rule <номер_правила> tcp mss
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
    rule номер_правила {
        tcp {
            mss значение
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

значение

Максимальный размер сегмента. Допустимые значения приведены в таблице ниже.

Таблица 123 - Допустимые значения максимального размера сегмента

Значение	Описание
<*x*>	Одиночное значение (где *x* - целое в диапазоне от *0* до *65535*)
<*x*>-<*y*>	Диапазон значений (где *x, y* - целое в диапазоне от *0* до *65535*, *x* < *y*)

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет проверять соответствие сетевых пакетов IPv6 критериям правила на основе указанного максимального размера сегмента. Предварительно должен быть определен протокол TCP для правила фильтрации при помощи команды *filter-ipv6 <имя> rule <номер_правила> protocol tcp*.

Форма **set** данной команды используется для указания максимального размера сегмента, на основе которых будет осуществляться проверка соответствия.

Форма **delete** данной команды позволяет восстановить поведение по умолчанию.

Форма **show** данной команды позволяет отобразить установленное в текущий момент значение максимального размера сегмента.

16.2.116 filter-ipv6 <имя> rule <номер_правила> tcp option <опция>

Указание опции TCP для проверки соответствия в правиле фильтрации трафика IPv6.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> tcp option <опция>
delete filter-ipv6 <имя> rule <номер_правила> tcp option
show filter-ipv6 <имя> rule <номер_правила> tcp option
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
    rule номер_правила {
        tcp {
            option опция
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

опция

Проверка на наличие/отсутствие указанной опции TCP в пакете. Допустимые значения приведены в таблице ниже.

Таблица 124 - Допустимые значения опции TCP

Значение	**Описание**
<x>	Номер опции TCP (где *x* - целое в диапазоне от *1* до *255*)
md5	Имитовставка с использованием алгоритма MD5 (номер 19)
mss	Максимальный размер сегмента (номер 2)
sack-permitted	Разрешение выборочного подтверждения (номер 4)
sack	Выборочное подтверждение (номер 5)
timestamp	Временная отметка (номер 8)
wscale	Масштабирование окна (номер 3)
!<y>	Проверка отсутствия заданной опции (*<y>* - любое значение, приведенное выше)

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет проверять наличие/отсутствие в сетевых пакетах указанной опции TCP. Предварительно должен быть определен протокол TCP для правила фильтрации при помощи команды *filter-ipv6 <имя> rule <номер_правила> protocol tcp*.

Форма **set** данной команды используется для указания опции, на основании которой будет осуществляться проверка соответствия.

Форма **delete** данной команды позволяет удалить заданное значение опции.

Форма **show** данной команды позволяет отобразить установленное в текущий момент значение проверяемой опции.

16.2.117 filter-ipv6 <имя> rule <номер_правила> time

Применение правил фильтрации трафика с учетом даты и времени.

Синтаксис

```
set filter-ipv6 <имя> rule <номер_правила> time [monthdays <дни_месяца> | startdate <дата> | starttime <время> | stopdate <дата> | stoptime <время> | utc | weekdays <дни_недели>]

delete filter-ipv6 <имя> rule <номер_правила>  time

show filter-ipv6 <имя> rule <номер_правила> time
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter-ipv6 имя {
    rule номер_правила {
        time {
            monthdays дни_месяца
            startdate дата
            starttime время
            stopdate дат
            stoptime время
            utc
```

```
            weekdays дни_недели
        }
    }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

дни_месяца

Дни месяца, в которые применяется указанное правило. Поддерживаются следующие значения: дни месяца (с 1 по 31), указанные через запятую (например, *3,15,24*). Может быть указан восклицательный знак ("!") для указания отрицания списка значений (например, *!3,15,24*). В данном случае правило фильтрации трафика будет применяться ежедневно, кроме указанных дней месяца.

startdate *дата*

Дата (и, в случае необходимости, время) начала периода действия правила. Указывается в следующем формате:

- **гггг-мм-дд** (например, 2020-04-21);
- **гггг-мм-ддТчч:мм:сс** (время, при необходимости указания, отделяется символом "T", например, 2020-04-21T16:45:00)

Время указывается в 24-часовом формате (значение должно находиться в диапазоне от 00:00:00 до 23:59:59). В том случае если время явно не указано, по умолчанию устанавливается начало указанного дня (т.е., 00:00:00). Для указания окончания периода действия правила используется параметр **stopdate**.

starttime *время*

Время начала периода, в течение которого правило будет применяться. Указывается в следующем формате:

- **чч:мм:сс** (например, 16:45:00).

Время указывается в 24-часовом формате (значение должно находиться в диапазоне от 00:00:00 до 23:59:59). Для указания времени окончания периода действия правила используется параметр **stoptime**.

stopdate *дата*

Дата (и, в случае необходимости, время) окончания периода действия правила. Указывается в следующем формате:

- **гггг-мм-дд** (например, 2020-04-21);
- **гггг-мм-ддТчч:мм:сс** (время, при необходимости указания, отделяется символом "T", например, 2020-04-21T16:45:00).

Время указывается в 24-часовом формате (значение должно находиться в диапазоне от 00:00:00 до 23:59:59). В том случае если время явно не указано, по умолчанию устанавливается начало указанного дня (т.е., 00:00:00). Для указания начала периода действия правила используется параметр **startdate**.

stoptime *время*

Время окончания периода, в течение которого правило будет применяться. Указывается в следующем формате:

- **чч:мм:сс**(например, 16:45:00).

Время указывается в 24-часовом формате (значение должно находиться в диапазоне от 00:00:00 до 23:59:59). Для указания времени начала периода действия правила используется параметр starttime.

utc

При указании данного параметра время, заданное при помощи параметров **startdate**, **stopdate**, **starttime**, и **stoptime**, должно быть интерпретировано как время UTC, а не как местное время.

дни_недели

Дни недели, по которым указанное правило будет применяться. Поддерживаются следующие значения: **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat** и **Sun**.

Дни недели могут быть указаны через запятую (например: **Mon**,**Wed**,**Fri**).

Для указания отрицания списка значений может быть указан восклицательный знак "!" (например, **!Mon**,**Wed**,**Fri**). В данном случае правило фильтрации трафика будет применяться ежедневно, кроме указанных дней недели.

Значение по умолчанию

Правило применяется постоянно без учета даты и времени.

Указания по использованию

Данная команда используется для ограничения времени, в течение которого применяется указанное правило фильтрации трафика.

Все параметры являются необязательными. В случае указания нескольких параметров объединяются логическим И.

Форма **set** данной команды используется для указания периода действия правила фильтрации трафика IPv6.

Форма **delete** данной команды используется для восстановления поведения по умолчанию.

Форма **show** данной команды используется для отображения настройки периода действия правила фильтрации трафика.

17 Политика модификации трафика

17.1 Обзор политик модификации трафика

Политики модификации трафика – это механизм, позволяющий изменять параметры пакетов, соответствующих критериям определённого фильтра, а именно:

- изменять значение поля DSCP;
- изменять максимальный размер сегмента TCP (MSS).

В настройках Numa Edge политики модификации трафика сгруппированы узлами **policy modify** для трафика IPv4 и **policy modify-ipv6** для трафика IPv6, которые служат контейнерами для операторов политики. Действующими операторами политики определяются правила модификации трафика. При этом модификация трафика, согласно определённой политике, производится только в случае её применения к конкретному интерфейсу и только для исходящего трафика.

Политики модификации трафика применяются последними перед отправкой данных: после маршрутизации, межсетевого экрана, применения фильтров QoS, но до непосредственной обработки QoS. Применение политик модификации трафика при прохождения трафика через Numa Edge показано на рисунке.

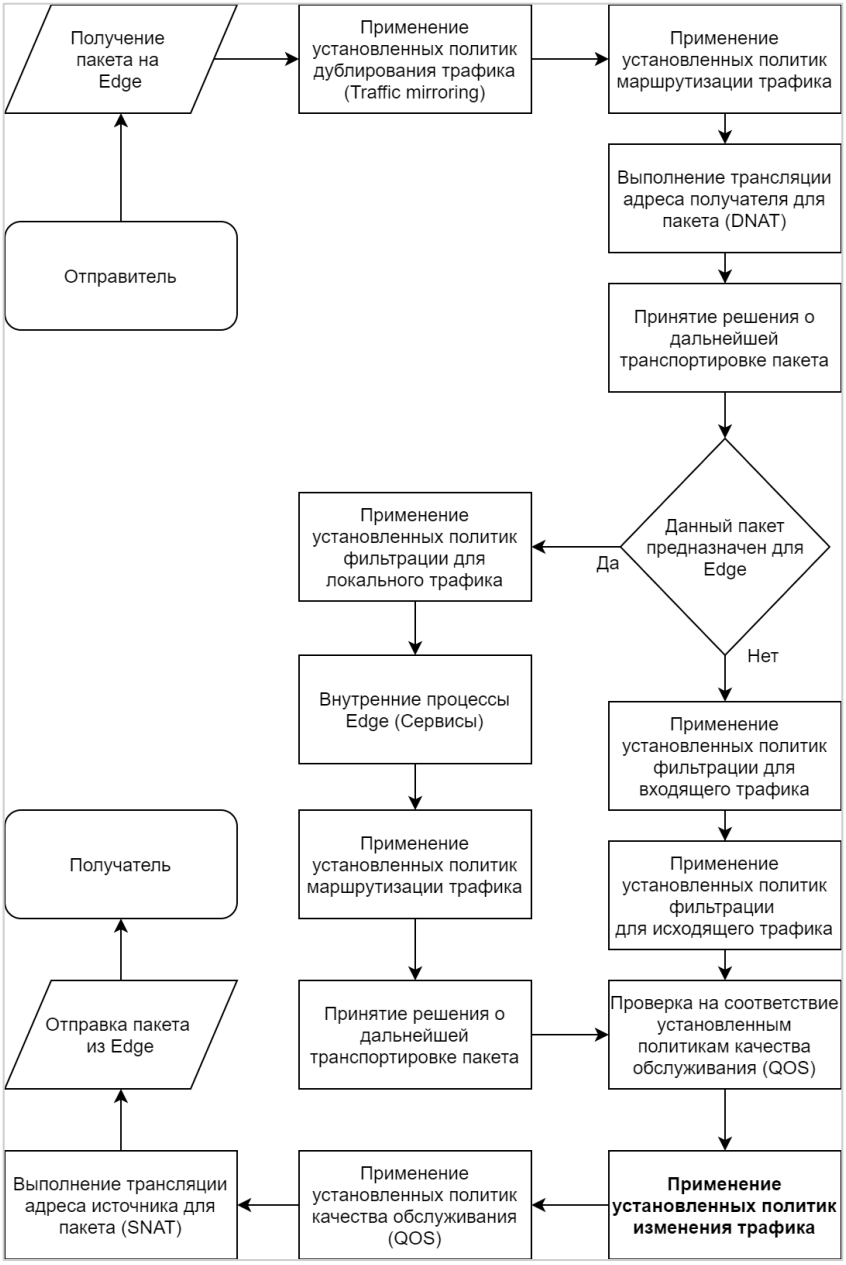


Рисунок 11 – Применение политик модификации трафика

Определённая политика модификации трафика применяется к определённому виртуальному или физическому интерфейсу.

17.2 Примеры настройки политик модификации трафика

В данном разделе приведены примеры настройки для политик маршрутизации. Рассматриваются следующие вопросы:

- Пример 133- Настройки политики модификации исходящего трафика с изменением значения поля DSCP
- Пример 134- Настройка политики модификации исходящего трафика с изменением максимального размера сегмента TCP (MSS)

17.2.1 Пример настройки политики модификации исходящего трафика с изменением значения поля DSCP

В примере выполняется настройка политики модификации трафика, передающегося по протоколам TCP или UDP, для которого порт источника пакета равен 5060 (порт по умолчанию для протокола SIP), на интерфейсе eth2 с изменением значения поля DSCP на значение, равное EF (ускоренная пересылка). Таким образом весь исходящий трафик, удовлетворяющий критериям, будет иметь малые задержками в очереди пересылки.

Для выполнения данной настройки необходимо выполнить следующую последовательность команд в режиме настройки.

Пример 133- Настройки политики модификации исходящего трафика с изменением значения поля DSCP

Действие	**Команда**
Создание фильтра SIP_filter.	`[edit]` `admin@edge# set filter SIP_filter`
Создание правила 10 для фильтра SIP_filter по определению атрибутов трафика протоколов TCP или UDP.	`[edit]` `admin@edge# set filter SIP_filter rule 10 protocol tcp_udp`
Указание порта источника пакета равного 5060 для правила 10 фильтра SIP_filter.	`[edit]` `admin@edge# set filter SIP_filter rule 10 source port 5060`
Фиксация настройки.	`[edit]` `admin@edge# commit`
Отображение настройки фильтра.	`[edit]` `admin@edge# show filter SIP_filter { rule 10 { protocol tcp_udp source { port 5060 } } }`
Создание в правиле 10 политики модификации трафика SIP_policy условия применения данной политики при совпадении атрибутов с указанными в фильтре SIP_filter.	`[edit]` `admin@edge# set policy modify SIP_policy rule 10 match filter SIP_filter`
Установка в правиле 10 политики модификации трафика SIP_policy изменения значения поля DSCP на значение, равное EF.	`[edit]` `admin@edge# set policy modify SIP_policy rule 10 set dscp EF`
Фиксация настройки.	`[edit]` `admin@edge# commit`
Отображение настройки политики модификации трафика.	`[edit]` `admin@edge# show policy modify SIP_policy { rule 10 { match { filter SIP_filter } set { dscp EF } } }`
Применение политики модификации трафика для исходящего трафика на интерфейсе `eth2`.	`[edit]` `admin@edge# set interfaces ethernet eth2 policy out modify SIP_policy`

Действие	Команда
Фиксация настройки.	[edit] admin@edge# commit
Отображение настройки применённых политик модификации трафика для интерфейса eth2.	[edit] admin@edge# show interfaces ethernet eth2 policy { out { modify SIP_policy } }

17.2.2 Пример настройки политики модификации исходящего трафика с изменением максимального размера сегмента TCP (MSS)

В примере 134 выполняется настройка политики модификации трафика, передающегося по протоколу TCP на интерфейсе eth1 с изменением значения максимального размера сегмента TCP (MSS) на значение, равное 1250 байт.

Для выполнения данной настройки необходимо выполнить следующую последовательность команд в режиме настройки.

Пример 134- Настройка политики модификации исходящего трафика с изменением максимального размера сегмента TCP (MSS)

Действие	Команда
Создание фильтра TCP_SYN_filter.	[edit] admin@edge# set filter TCP_SYN_filter
Создание правила 10 для фильтра TCP_SYN_filter по определению атрибутов трафика протокола TCP.	[edit] admin@edge# set filter TCP_SYN_filter rule 10 protocol tcp
Установка флага TCP SYN для правила 10 фильтра TCP_SYN_filter.	[edit] admin@edge# set filter TCP_SYN_filter rule 10 tcp flags SYN
Фиксация настройки.	[edit] admin@edge# commit

Отображение настройки фильтра.	[edit]
	admin@edge# show filter
	TCP_SYN_filter {
	rule 10 {
	protocol tcp
	tcp {
	flags SYN
	}
	}
	}

Создание в правиле 10 политики модификации трафика MSS_modify_policy условия применения данной политики при совпадении атрибутов с указанными в фильтре TCP_SYN_filter.	[edit] admin@edge# set policy modify MSS_modify_policy rule 10 match filter TCP_SYN_filter
Установка в правиле 10 политики модификации трафика MSS_modify_policy изменения значения максимального размера сегмента TCP (MSS) на значение, равное 1250 байт.	[edit] admin@edge# set policy modify MSS_modify_policy rule 10 set tcp-mss 1250
Фиксация настройки.	[edit] admin@edge# commit
Отображение настройки политики модификации трафика.	[edit] admin@edge# show policy modify MSS_modify_policy { rule 10 { match { filter TCP_SYN_filter } set { tcp-mss 1250 } } }

Действие	Команда
Применение политики модификации трафика для исходящего трафика на интерфейсе `eth1`.	`[edit]` `admin@edge# set interfaces ethernet eth1 policy out modify MSS_modify_policy`
Фиксация настройки.	`[edit]` `admin@edge# commit`
Отображение настройки применённых политик модификации трафика для интерфейса `eth1`.	`[edit]` `admin@edge# show interfaces ethernet eth1 policy { out { modify MSS_modify_policy } }`

17.3 Команды политик модификации трафика

Команды настройки	
Применение политик модификации IPv4-трафика к интерфейсам	
interfaces <интерфейс> policy out modify <имя_политики>	Применение политики модификации IPv4-трафика к указанному интерфейсу.
Применение политик модификации IPv6-трафика к интерфейсам	
interfaces <интерфейс> policy out modify-ipv6 <имя_политики>	Применение политики модификации IPv6-трафика к указанному интерфейсу.
Команды настройки политик модификации трафика для протокола IPv4	
policy modify <имя_политики>	Определение политики модификации IPv4-трафика.
policy modify <имя_политики> description <описание>	Создание текстового описания для указанной политики модификации IPv4-трафика.
policy modify <имя_политики> rule <номер_правила> description <описание>	Задание текстового описания для правила в указанной политики модификации IPv4-трафика.
policy modify <имя_политики> rule <номер_правила> log <состояние>	Включение/выключение регистрации событий модификации пакетов IPv4 для указанного правила политики.
policy modify <имя_политики> rule <номер_правила> match filter <имя_фильтра>	Определение условия соответствия IPv4-трафика определённому фильтру.
policy modify <имя_политики> rule <номер_правила> set dscp <значение>	Установка значения поля DSCP в заголовке пакета, для которого установлено соответствие критериям определённого фильтра.
policy modify <имя_политики> rule <номер_правила> set tcp-mss <значение>	Установка значения максимального размера сегмента TCP (MSS) в заголовке пакета, для которого установлено соответствие критериям определённого фильтра.
policy modify <имя_политики> rule <номер_правила> strip tcp-option <значение>	Удаление опций протокола TCP в заголовке пакета, для которого установлено соответствие критериям определённого фильтра.
Команды настройки политик модификации трафика для протокола IPv6	
policy modify-ipv6 <имя_политики>	Определение политики модификации IPv6-трафика.
policy modify-ipv6 <имя_политики> description <описание>	Создание текстового описания для указанной политики модификации IPv6-трафика.
policy modify-ipv6 <имя_политики> rule <номер_правила> description <описание>	Задание текстового описания для правила в указанной политики модификации IPv6-трафика.
policy modify-ipv6 <имя_политики> rule <номер_правила> log <состояние>	Включение/выключение регистрации событий модификации пакетов IPv6 для указанного правила политики.
policy modify-ipv6 <имя_политики> rule <номер_правила> match filter-ipv6 <имя_фильтра>	Определение условия соответствия IPv6-трафика определённому фильтру.
policy modify-ipv6 <имя_политики> rule <номер_правила> set dscp <значение>	Установка значения поля DSCP в заголовке пакета, для которого установлено соответствие критериям определённого фильтра.
policy modify-ipv6 <имя_политики> rule <номер_правила> set tcp-mss <значение>	Установка значения максимального размера сегмента TCP (MSS) в заголовке пакета, для которого установлено

	соответствие критериям определённого фильтра.
policy modify-ipv6 <имя_политики> rule <номер_правила> strip tcp-option <значение>	Удаление опций протокола TCP в заголовке пакета, для которого установлено соответствие критериям определённого фильтра.
Эксплуатационные команды	
Эксплуатационные команды IPv4	
policy clear modify <имя_политики>	Очистка статистики для указанной политики модификации IPv4-трафика.
policy clear modify <имя_политики> rule <номер_правила>	Очистка статистики для правила указанной политики модификации IPv4-трафика.
policy clear modify <имя_политики> rule <номер_правила> filter	Очистка статистики для фильтра, связанного с указанным правилом политики модификации IPv4-трафика.
policy clear modify <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>	Очистка статистики для указанного правила фильтра, связанного с указанным правилом политики модификации IPv4-трафика.
policy show modify <имя_политики>	Вывод сведений и статистики для указанной политики модификации IPv4-трафика.
policy show modify <имя_политики> rule <номер_правила>	Вывод сведений и статистики для правила указанной политики модификации IPv4-трафика.
policy show modify <имя_политики> rule <номер_правила> filter	Вывод статистики для фильтра, связанного с указанным правилом политики модификации IPv4-трафика.
policy show modify <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>	Вывод статистики для указанного правила фильтра, связанного с указанным правилом политики модификации IPv4-трафика.
Эксплуатационные команды IPv6	
policy clear modify-ipv6 <имя_политики>	Очистка статистики для указанной политики модификации IPv6-трафика.
policy clear modify-ipv6 <имя_политики> rule <номер_правила>	Очистка статистики для правила указанной политики модификации IPv6-трафика.
policy clear modify-ipv6 <имя_политики> rule <номер_правила> filter	Очистка статистики для фильтра, связанного с указанным правилом политики модификации IPv6-трафика.
policy clear modify-ipv6 <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>	Очистка статистики для указанного правила фильтра, связанного с указанным правилом политики модификации IPv6-трафика.
policy show modify-ipv6 <имя_политики>	Вывод сведений и статистики для указанной политики модификации IPv6-трафика.
policy show modify-ipv6 <имя_политики> rule <номер_правила>	Вывод сведений и статистики для правила указанной политики модификации IPv6-трафика.
policy show modify-ipv6 <имя_политики> rule <номер_правила> filter	Вывод статистики для фильтра, связанного с указанным правилом политики модификации IPv6-трафика.
policy show modify-ipv6 <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>	Вывод статистики для указанного правила фильтра, связанного с указанным правилом политики модификации IPv6-трафика.

17.3.1 interfaces <интерфейс> policy out modify <имя_политики>

Применение политики модификации IPv4-трафика к указанному интерфейсу.

Синтаксис

```
set interfaces <интерфейс> policy out modify <имя_политики>
delete interfaces <интерфейс> policy out modify <имя_политики>
show interfaces <интерфейс> policy out modify
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   интерфейс {
      policy {
         out {
            modify имя_политики
         }
      }
   }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже в разделе Указания по использованию.

имя_политики

Имя политики модификации трафика, применяемой к данному интерфейсу.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для применения политики модификации IPv4-трафика к интерфейсу.

В приведенной ниже таблице показаны типы поддерживаемых интерфейсов и синтаксис.

Таблица 125 – Типы интерфейсов

Тип интерфейса	Синтаксис
Агрегирование каналов	bonding bondx
Виртуальный интерфейс агрегированных каналов	bonding bondx vif идентификатор_vlan
Сетевой мост	bridge brx
Ethernet	ethernet ethx
Ethernet PPPoE	ethernet ethx pppoe номер
Виртуальный интерфейс Ethernet	ethernet ethx vif идентификатор_vlan
Ethernet Vif PPPoE	ethernet ethx vif идентификатор_vlan pppoe номер
Интерфейс заглушки	loopback lo
Многоканальная связь	multilink mlx
OpenVPN	openvpn vtunx
Псевдо-Ethernet	pseudo-ethernet pethx
Последовательный интерфейс	serial srx vif идентификатор_vlan
Туннель	tunnel tunx

Форма **set** данной команды используется для применения политики модификации трафика к интерфейсу.

Форма **delete** данной команды используется для удаления политики модификации трафика с интерфейса.

Форма **show** данной команды используется для отображения настройки политики модификации трафика на интерфейсе.

17.3.2 interfaces <интерфейс> policy out modify-ipv6 <имя_политики>

Применение политики модификации IPv6-трафика к указанному интерфейсу.

Синтаксис

```
set interfaces <интерфейс> policy out modify-ipv6 <имя_политики>
```

```
delete interfaces <интерфейс> policy out modify-ipv6 <имя_политики>
show interfaces <интерфейс> policy out modify-ipv6
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   интерфейс {
      policy {
         out {
            modify-ipv6 имя_политики
         }
      }
   }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже в разделе Указания по использованию.

имя_политики

Имя политики модификации трафика, применяемой к данному интерфейсу.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для применения политики модификации IPv6-трафика к интерфейсу.

В приведенной ниже таблице показаны типы поддерживаемых интерфейсов и синтаксис.

Таблица 126 – Типы интерфейсов

Тип интерфейса	Синтаксис
Агрегирование каналов	bonding bondx
Виртуальный интерфейс агрегированных каналов	bonding bondx vif идентификатор_vlan
Сетевой мост	bridge brx
Ethernet	ethernet ethx
Ethernet PPPoE	ethernet ethx pppoe номер
Виртуальный интерфейс Ethernet	ethernet ethx vif идентификатор_vlan
Ethernet Vif PPPoE	ethernet ethx vif идентификатор_vlan pppoe номер
Интерфейс заглушки	loopback lo
Многоканальная связь	multilink mlx
OpenVPN	openvpn vtunx
Псевдо-Ethernet	pseudo-ethernet pethx
Последовательный интерфейс	serial srx vif идентификатор_vlan
Туннель	tunnel tunx

Форма **set** данной команды используется для применения политики модификации трафика к интерфейсу.

Форма **delete** данной команды используется для удаления политики модификации трафика с интерфейса.

Форма **show** данной команды используется для отображения настройки политики модификации трафика на интерфейсе.

17.3.3 policy modify <имя_политики>

Определение политики модификации IPv4-трафика.

Синтаксис

```
set policy modify <имя_политики>
delete policy modify <имя_политики>
show policy modify <имя_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   modify имя_политики {
  }
}
```

Параметры

имя_политики

Имя политики модификации IPv4-трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет создать политику модификации трафика.

Форма **set** данной команды используется для определения политики модификации трафика.

Форма **delete** данной команды используется для удаления политики модификации трафика.

Форма **show** данной команды используется для отображения политики модификации трафика.

17.3.4 policy modify <имя_политики> description <описание>

Создание текстового описания для указанной политики модификации IPv4-трафика.

Синтаксис

```
set policy modify <имя_политики> description <описание>
delete policy modify <имя_политики> description
show policy modify <имя_политики> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   modify имя_политики {
      description описание
   }
}
```

Параметры

имя_политики

Имя политики модификации IPv4-трафика.

описание

Текстовое описание политики. В том случае если описание содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для задания текстового описания для указанной политики.

Форма **delete** используется для удаления описания.

Форма **show** используется для отображения описания.

17.3.5 policy modify <имя_политики> rule <номер_правила> description <описание>

Задание текстового описания для правила в указанной политики модификации IPv4-трафика.

Синтаксис

```
set policy modify <имя_политики> rule <номер_правила> description <описание>
delete policy modify <имя_политики> rule <номер_правила> description
show policy modify <имя_политики> rule <номер_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   modify имя_политики {
      rule номер_правила {
         description описание
      }
   }
}
```

Параметры

имя_политики

Имя политики модификации IPv4-трафика.

описание

Текстовое описание политики. В том случае если описание содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для задания текстового описания для указанной политики.

Форма **delete** используется для удаления описания.

Форма **show** используется для отображения описания.

17.3.6 policy modify <имя_политики> rule <номер_правила> log <состояние>

Включение/выключение регистрации событий модификации пакетов IPv4 для указанного правила политики.

Синтаксис

```
set policy modify <имя_политики> rule <номер_правила> log <состояние>
delete policy modify <имя_политики> rule <номер_правила> log
```

```
show policy modify <имя_политики> rule <номер_правила> log
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   modify имя_политики {
      rule номер_правила {
         log состоояние
      }
   }
}
```

Параметры

имя_политики

Имя политики модификации IPv4-трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно находиться в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации **rule**.

состояние

Указывает режим регистрации событий для правил политики. Допустимые значения:

enable: Включение регистрации событий для правила политики;

disable: Отключение регистрации событий для правила политики.

Значение по умолчанию

Отсутствует.

Указания по использованию

При включенной регистрации событий для правила политики в системный журнал будут выводиться сообщения для всех пакетов, удовлетворяющих правилу. Для каждого сообщения формируется префикс в квадратных скобках **[m-**<*имя_политики*>**-**<*номер_правила*>**]**. Имя политики (<*имя_политики*>) может быть записано в журнале не полностью в связи с системным ограничением общей длины префикса в 16 символов.

Форма **set** данной команды используется для задания настройки регистрации событий модификации трафика.

Форма **delete** данной команды используется для удаления настройки регистрации событий модификации трафика.

Форма **show** данной команды используется для отображения настройки регистрации событий модификации трафика.

17.3.7 policy modify <имя_политики> rule <номер_правила> match filter <имя_фильтра>

Определение условия соответствия IPv4-трафика определённому фильтру.

Синтаксис

```
set policy modify <имя_политики> rule <номер_правила> match filter
<имя_фильтра>

delete policy modify <имя_политики> rule <номер_правила> match filter
<имя_фильтра>

show policy modify <имя_политики> rule <номер_правила> match filter
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   modify имя_политики {
      rule номер_правила {
         match {
            filter имя_фильтра
         }
      }
   }
}
```

Параметры

имя_политики

Имя политики модификации IPv4-трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно находиться в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации **rule**.

имя_фильтра

Имя фильтра IPv4-трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для определения условия соответствия IPv4-трафика определённому фильтру. Фильтр IPv4-трафика должен быть предварительно определен при помощи команды *filter <имя_фильтра>*. Для одного правила может быть указан только один фильтр. Проверка пакетов выполняется на соответствие их атрибутов параметрам фильтра трафика.

Форма **set** данной команды используется для определения условия соответствия трафика определённому фильтру.

Форма **delete** данной команды используется для удаления условия соответствия трафика определённому фильтру.

Форма **show** данной команды используется для отображения настройки условия соответствия трафика определённому фильтру.

17.3.8 policy modify <имя_политики> rule <номер_правила> set dscp <значение>

Установка значения поля DSCP в заголовке пакета, для которого установлено соответствие критериям определённого фильтра.

Синтаксис

```
set policy modify <имя_политики> rule <номер_правила> set dscp <значение>
delete policy modify <имя_политики> rule <номер_правила> set dscp <значение>
show policy modify <имя_политики> rule <номер_правила> set dscp
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   modify имя_политики {
      rule номер_правила {
         set {
            dscp значение
         }
      }
   }
}
```

Параметры

имя_политики

Имя политики модификации IPv4-трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно находиться в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации **rule**.

значение

Данное значение записывается в поле DSCP пакетов трафика, соответствующего критериям определённого фильтра. Допустимые значения приведены в таблице ниже.

Таблица 127 - Допустимые значения поля DSCP

Значение	Описание
<x>	Численное значение DSCP (где x - десятичное значение в диапазоне от 0 до 63)
<x>	Численное значение DSCP (где x - шестнадцатеричное значения в диапазоне от 0 до 3F в формате 0xYZ, например, 0x2E или 0x2e)
default	Значение DSCP по умолчанию, соответствующее стандартной пересылке (шестнадцатеричное значение - 0x0, двоичное значение - 000000)
EF	Значение Express Forwarding, соответствующее экстренной пересылке
AFxy	Значение Assured Forwarding, соответствующее гарантированной пересылке (x находится в диапазоне от 1 до 4, y - от 1 до 3)
CSx	Значение Class Selector поддерживает обратную совместимость с полем приоритета IP (x находится в диапазоне от 1 до 7)

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для установки значения поля DSCP в заголовке пакета трафика, соответствующего критериям определённого фильтра. Изменение значения поля DSCP позволяет осуществлять управление трафиком и обеспечение качества обслуживания.

Форма **set** данной команды используется для определения значения поля DSCP IPv4-трафика.

Форма **delete** данной команды используется для удаления значения поля DSCP IPv4-трафика.

Форма **show** данной команды используется для отображения значения поля DSCP IPv4-трафика.

17.3.9 policy modify <имя_политики> rule <номер_правила> set tcp-mss <значение>

Установка значения максимального размера сегмента TCP (MSS) в заголовке пакета, для которого установлено соответствие критериям определённого фильтра.

Синтаксис

```
set policy modify <имя_политики> rule <номер_правила> set tcp-mss <значение>

delete policy modify <имя_политики> rule <номер_правила> set tcp-mss <значение>

show policy modify <имя_политики> rule <номер_правила> set tcp-mss
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    modify имя_политики {
        rule номер_правила {
            set {
                tcp-mss значение
            }
        }
    }
}
```

Параметры

имя_политики

Имя политики модификации IPv4-трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно находиться в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации **rule**.

значение

Значение максимального размера сегмента TCP (MSS). Допустимые значения:

pmtu: Значение TCP MSS равное значению PMTU минус 40 байт;

<x>: Числовое значение TCP MSS (x находится в диапазоне от 500 до 8960).

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для установки значения максимального размера сегмента TCP (MSS) в заголовке пакета трафика, соответствующего критериям определённого фильтра.

Форма **set** данной команды используется для определения значения TCP MSS IPv4-трафика.

Форма **delete** данной команды используется для удаления значения TCP MSS IPv4-трафика.

Форма **show** данной команды используется для отображения значения TCP MSS IPv4-трафика.

17.3.10 policy modify <имя_политики> rule <номер_правила> strip tcp-option <значение>

Удаление опций протокола TCP в заголовке пакета, для которого установлено соответствие критериям определённого фильтра.

Синтаксис

```
set policy modify <имя_политики> rule <номер_правила> strip tcp-option <значение>

delete policy modify <имя_политики> rule <номер_правила> strip tcp-option <значение>

show policy modify <имя_политики> rule <номер_правила> strip tcp-option
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   modify имя_политики {
      rule номер_правила {
         strip {
            tcp-option значение
         }
      }
   }
}
```

Параметры

имя_политики

Имя политики модификации IPv4-трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно находиться в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации **rule**.

значение

Значение опции протокола TCP в заголовке пакета. Допустимые значения приведены в таблице ниже.

Таблица 128 - Допустимые значения опций протокола TCP

Значение	Описание
<x>	Номер опции TCP (*x* находится в диапазоне от *2* до *255*)
md5	Имитовставка с использованием алгоритма MD5 (номер 19)
mss	Максимальный размер сегмента (номер 2)
sack-permitted	Разрешение выборочного подтверждения (номер 4)
sack	Выборочное подтверждение (номер 5)
timestamp	Временная отметка (номер 8)
wscale	Масштабирование окна (номер 3)

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания опции протокола TCP в заголовке пакета, соответствующего критериям определённого фильтра, которая должна быть удалена. Допустимо одновременное указание нескольких опций протокола TCP.

Форма **set** данной команды используется для определения значения опции протокола TCP.

Форма **delete** данной команды используется для удаления значения опции протокола TCP.

Форма **show** данной команды используется для отображения значения опции протокола TCP.

17.3.11 policy modify-ipv6 <имя_политики>

Определение политики модификации IPv6-трафика.

Синтаксис

```
set policy modify-ipv6 <имя_политики>
delete policy modify-ipv6 <имя_политики>
show policy modify-ipv6 <имя_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   modify-ipv6 имя_политики {
   }
}
```

Параметры

имя_политики

Имя политики модификации IPv6-трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет создать политику модификации трафика.

Форма **set** данной команды используется для определения политики модификации трафика.

Форма **delete** данной команды используется для удаления политики модификации трафика.

Форма **show** данной команды используется для отображения политики модификации трафика.

17.3.12 policy modify-ipv6 <имя_политики> description <описание>

Создание текстового описания для указанной политики модификации IPv6-трафика.

Синтаксис

```
set policy modify-ipv6 <имя_политики> description <описание>
delete policy modify-ipv6 <имя_политики> description
show policy modify-ipv6 <имя_политики> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   modify-ipv6 имя_политики {
      description описание
   }
}
```

Параметры

имя_политики

Имя политики модификации IPv6-трафика.

описание

Текстовое описание политики. В том случае если описание содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для задания текстового описания для указанной политики.

Форма **delete** используется для удаления описания.

Форма **show** используется для отображения описания.

17.3.13 policy modify-ipv6 <имя_политики> rule <номер_правила> description <описание>

Задание текстового описания для правила в указанной политики модификации IPv6-трафика.

Синтаксис

```
set policy modify-ipv6 <имя_политики> rule <номер_правила> description <описание>
delete policy modify-ipv6 <имя_политики> rule <номер_правила> description
show policy modify-ipv6 <имя_политики> rule <номер_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   modify-ipv6 имя_политики {
      rule номер_правила {
         description описание
      }
   }
}
```

Параметры

имя_политики

Имя политики модификации IPv6-трафика.

описание

Текстовое описание политики. В том случае если описание содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для задания текстового описания для указанной политики.

Форма **delete** используется для удаления описания.

Форма **show** используется для отображения описания.

17.3.14 policy modify-ipv6 <имя_политики> rule <номер_правила> log <состояние>

Включение/выключение регистрации событий модификации пакетов IPv6 для указанного правила политики.

Синтаксис

```
set policy modify-ipv6 <имя_политики> rule <номер_правила> log <состояние>
delete policy modify-ipv6 <имя_политики> rule <номер_правила> log
ырщц зщдшсн ьщвшан-шзм6 Бимя_политикиЮ кгду Бномер_правилаЮ дщп
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   modify-ipv6 имя_политики {
      rule номер_правила {
         log состояние
      }
   }
}
```

Параметры

имя_политики

Имя политики модификации IPv6-трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно находиться в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации **rule**.

состояние

Указывает режим регистрации событий для правил политики. Допустимые значения:

enable: Включение регистрации событий для правила политики;

disable: Отключение регистрации событий для правила политики.

Значение по умолчанию

Отсутствует.

Указания по использованию

При включенной регистрации событий для правила политики в системный журнал будут выводиться сообщения для всех пакетов, удовлетворяющих правилу. Для каждого сообщения формируется префикс в квадратных скобках **[m6-**<имя_политики>-<номер_правила>**]**. Имя политики (*<имя_политики>*) может быть записано в журнале не полностью в связи с системным ограничением общей длины префикса в 16 символов.

Форма **set** данной команды используется для задания настройки регистрации событий модификации трафика.

Форма **delete** данной команды используется для удаления настройки регистрации событий модификации трафика.

Форма **show** данной команды используется для отображения настройки регистрации событий модификации трафика.

17.3.15 policy modify-ipv6 <имя_политики> rule <номер_правила> match filter-ipv6 <имя_фильтра>

Определение условия соответствия IPv6-трафика определённому фильтру.

Синтаксис

```
set policy modify-ipv6 <имя_политики> rule <номер_правила> match filter-ipv6 <имя_фильтра>

delete policy modify-ipv6 <имя_политики> rule <номер_правила> match filter-ipv6 <имя_фильтра>

show policy modify-ipv6 <имя_политики> rule <номер_правила> match filter-ipv6
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    modify-ipv6 имя_политики {
        rule номер_правила {
            match {
                filter-ipv6 имя_фильтра
            }
        }
    }
}
```

Параметры

имя_политики

Имя политики модификации IPv6-трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно находиться в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации **rule**.

имя_фильтра

Имя фильтра IPv6-трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для определения условия соответствия IPv6-трафика определённому фильтру. Фильтр IPv6-трафика должен быть предварительно определен при помощи команды *filter-ipv6 <имя_фильтра>*. Для одного правила может быть указан только один фильтр. Проверка пакетов выполняется на соответствие их атрибутов параметрам фильтра трафика.

Форма **set** данной команды используется для определения условия соответствия трафика определённому фильтру.

Форма **delete** данной команды используется для удаления условия соответствия трафика определённому фильтру.

Форма **show** данной команды используется для отображения настройки условия соответствия трафика определённому фильтру.

17.3.16 policy modify-ipv6 <имя_политики> rule <номер_правила> set dscp <значение>

Установка значения поля DSCP в заголовке пакета, для которого установлено соответствие критериям определённого фильтра.

Синтаксис

```
set policy modify-ipv6 <имя_политики> rule <номер_правила> set tcp-mss <значение>

delete policy modify-ipv6 <имя_политики> rule <номер_правила> set tcp-mss <значение>

show policy modify-ipv6 <имя_политики> rule <номер_правила> set tcp-mss
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   modify-ipv6 имя_политики {
      rule номер_правила {
         set {
            tcp-mss значение
         }
      }
   }
}
```

Параметры

имя_политики

Имя политики модификации IPv6-трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно находиться в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации **rule**.

значение

Данное значение записывается в поле DSCP пакетов трафика, соответствующего критериям определённого фильтра. Допустимые значения приведены в таблице ниже.

Таблица 129 - Допустимые значения поля DSCP

Значение	Описание
<x>	Численное значение DSCP (где *x* - десятичное значение в диапазоне от *0* до *63*)
<x>	Численное значение DSCP (где *x* - шестнадцатеричное значения в диапазоне от *0* до *3F* в формате *0xYZ*, например, *0x2E* или *0x2e*)
default	Значение DSCP по умолчанию, соответствующее стандартной пересылке (шестнадцатеричное значение - *0x0*, двоичное значение - *000000*)
EF	Значение Express Forwarding, соответствующее экстренной пересылке
AFxy	Значение Assured Forwarding, соответствующее гарантированной пересылке (*x* находится в диапазоне от *1* до *4*, y - от *1* до *3*)
CSx	Значение Class Selector поддерживает обратную совместимость с полем приоритета IP (*x* находится в диапазоне от *1* до *7*)

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для установки значения поля DSCP в заголовке пакета трафика, соответствующего критериям определённого фильтра. Изменение значения поля DSCP позволяет осуществлять управление трафиком и обеспечение качества обслуживания.

Форма **set** данной команды используется для определения значения поля DSCP IPv6-трафика.

Форма **delete** данной команды используется для удаления значения поля DSCP IPv6-трафика.

Форма **show** данной команды используется для отображения значения поля DSCP IPv6-трафика.

17.3.17 policy modify-ipv6 <имя_политики> rule <номер_правила> set tcp-mss <значение>

Установка значения максимального размера сегмента TCP (MSS) в заголовке пакета, для которого установлено соответствие критериям определённого фильтра.

Синтаксис

```
set policy modify-ipv6 <имя_политики> rule <номер_правила> set tcp-mss <значение>

delete policy modify-ipv6 <имя_политики> rule <номер_правила> set tcp-mss <значение>

show policy modify-ipv6 <имя_политики> rule <номер_правила> set tcp-mss
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    modify-ipv6 имя_политики {
        rule номер_правила {
            set {
                tcp-mss значение
            }
        }
    }
}
```

Параметры

имя_политики

Имя политики модификации IPv6-трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно находиться в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации **rule**.

значение

Значение максимального размера сегмента TCP (MSS). Допустимые значения:

pmtu: Значение TCP MSS равное значению PMTU минус 40 байт;

<x>: Числовое значение TCP MSS (x находится в диапазоне от 500 до 8960).

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для установки значения максимального размера сегмента TCP (MSS) в заголовке пакета трафика, соответствующего критериям определённого фильтра.

Форма **set** данной команды используется для определения значения TCP MSS IPv6-трафика.

Форма **delete** данной команды используется для удаления значения TCP MSS IPv6-трафика.

Форма **show** данной команды используется для отображения значения TCP MSS IPv6-трафика.

17.3.18 policy modify-ipv6 <имя_политики> rule <номер_правила> strip tcp-option <значение>

Удаление опций протокола TCP в заголовке пакета, для которого установлено соответствие критериям определённого фильтра.

Синтаксис

```
set policy modify-ipv6 <имя_политики> rule <номер_правила> strip tcp-option <значение>
```

```
delete policy modify-ipv6 <имя_политики> rule <номер_правила> strip tcp-option <значение>
```

```
show policy modify-ipv6 <имя_политики> rule <номер_правила> strip tcp-option
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    modify-ipv6 имя_политики {
        rule номер_правила {
            strip {
                tcp-option значение
            }
        }
    }
}
```

Параметры

имя_политики

Имя политики модификации IPv4-трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно находиться в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации **rule**.

значение

Значение опции протокола TCP в заголовке пакета. Допустимые значения приведены в таблице ниже.

Таблица 130 - Допустимые значения опций протокола TCP

Значение	Описание
<x>	Номер опции TCP (*x* находится в диапазоне от *2* до *255*)
md5	Имитовставка с использованием алгоритма MD5 (номер 19)
mss	Максимальный размер сегмента (номер 2)
sack-permitted	Разрешение выборочного подтверждения (номер 4)

sack	Выборочное подтверждение (номер 5)
timestamp	Временная отметка (номер 8)
wscale	Масштабирование окна (номер 3)

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания опции протокола TCP в заголовке пакета, соответствующего критериям определённого фильтра, которая должна быть удалена. Допустимо одновременное указание нескольких опций протокола TCP.

Форма **set** данной команды используется для определения значения опции протокола TCP.

Форма **delete** данной команды используется для удаления значения опции протокола TCP.

Форма **show** данной команды используется для отображения значения опции протокола TCP.

17.3.19 policy clear modify <имя_политики>

Очистка статистики для указанной политики модификации IPv4-трафика.

Синтаксис

```
policy clear modify <имя_политики>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики модификации IPv4-трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для очистки статистики указанной политики модификации IPv4-трафика.

17.3.20 policy clear modify <имя_политики> rule <номер_правила>

Очистка статистики для правила указанной политики модификации IPv4-трафика.

Синтаксис

```
policy clear modify <имя_политики> rule <номер_правила>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики модификации IPv4-трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 65535.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для очистки статистики для правила указанной политики модификации IPv4-трафика.

17.3.21 policy clear modify <имя_политики> rule <номер_правила> filter

Очистка статистики для фильтра, связанного с указанным правилом политики модификации IPv4-трафика.

Синтаксис

```
policy clear modify <имя_политики> rule <номер_правила> filter
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики модификации IPv4-трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 65535.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для очистки статистики для фильтра, связанного с указанным правилом политики модификации IPv4-трафика.

17.3.22 policy clear modify <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>

Очистка статистики для указанного правила фильтра, связанного с указанным правилом политики модификации IPv4-трафика.

Синтаксис

```
policy clear modify <имя_политики> rule <номер_правила> filter rule
<номер_правила_фильтра>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики модификации IPv4-трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 65535.

номер_правила_фильтра

Численный идентификатор правила фильтра. Значение должно лежать в диапазоне от 1 до 9999.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для очистки статистики для указанного правила фильтра, связанного с указанным правилом политики модификации IPv4-трафика.

17.3.23 policy show modify <имя_политики>

Вывод сведений и статистики для указанной политики модификации IPv4-трафика.

Синтаксис

```
policy show modify <имя_политики>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики модификации IPv4-трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения сведений и статистики для указанной политики модификации IPv4-трафика. Так же выводятся сведения об интерфейсах, к которым применена указанная политика.

17.3.24 policy show modify <имя_политики> rule <номер_правила>

Вывод сведений и статистики для правила указанной политики модификации IPv4-трафика.

Синтаксис

```
policy show modify <имя_политики> rule <номер_правила>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики модификации IPv4-трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 65535.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения сведений и статистики для правила указанной политики модификации IPv4-трафика. Так же выводятся сведения об интерфейсах, к которым применена указанная политика.

17.3.25 policy show modify <имя_политики> rule <номер_правила> filter

Вывод статистики для фильтра, связанного с указанным правилом политики модификации IPv4-трафика.

Синтаксис

```
policy show modify <имя_политики> rule <номер_правила> filter [detail]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики модификации IPv4-трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 65535.

detail

Вывод подробных сведений.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения статистики для фильтра, связанного с указанным правилом политики модификации IPv4-трафика. Если в фильтре присутствует несколько правил, то статистика выводится по каждому правилу отдельно.

17.3.26 policy show modify <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>

Вывод статистики для указанного правила фильтра, связанного с указанным правилом политики модификации IPv4-трафика.

Синтаксис

```
policy show modify <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра> [detail]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики модификации IPv4-трафика./

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 65535.

номер_правила_фильтра

Численный идентификатор правила фильтра. Значение должно лежать в диапазоне от 1 до 9999.

detail

Вывод подробных сведений.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения статистики для указанного правила фильтра, связанного с указанным правилом политики модификации IPv4-трафика.

17.3.27 policy clear modify-ipv6 <имя_политики>

Очистка статистики для указанной политики модификации IPv6-трафика.

Синтаксис

```
policy clear modify-ipv6 <имя_политики>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики модификации IPv6-трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для очистки статистики указанной политики модификации IPv6-трафика.

17.3.28 policy clear modify-ipv6 <имя_политики> rule <номер_правила>

Очистка статистики для правила указанной политики модификации IPv6-трафика.

Синтаксис

```
policy clear modify-ipv6 <имя_политики> rule <номер_правила>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики модификации IPv6-трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 65535.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для очистки статистики для правила указанной политики модификации IPv6-трафика.

17.3.29 policy clear modify-ipv6 <имя_политики> rule <номер_правила> filter

Очистка статистики для фильтра, связанного с указанным правилом политики модификации IPv6-трафика.

Синтаксис

```
policy clear modify-ipv6 <имя_политики> rule <номер_правила> filter
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики модификации IPv6-трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 65535.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для очистки статистики для фильтра, связанного с указанным правилом политики модификации IPv6-трафика.

17.3.30 policy clear modify-ipv6 <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>

Очистка статистики для указанного правила фильтра, связанного с указанным правилом политики модификации IPv6-трафика.

Синтаксис

```
policy clear modify-ipv6 <имя_политики> rule <номер_правила> filter rule
<номер_правила_фильтра>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики модификации IPv6-трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 65535.

номер_правила_фильтра

Численный идентификатор правила фильтра. Значение должно лежать в диапазоне от 1 до 9999.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для очистки статистики для указанного правила фильтра, связанного с указанным правилом политики модификации IPv6-трафика.

17.3.31 policy show modify-ipv6 <имя_политики>

Вывод сведений и статистики для указанной политики модификации IPv6-трафика.

Синтаксис

```
policy show modify-ipv6 <имя_политики>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики модификации IPv6-трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения сведений и статистики для указанной политики модификации IPv6-трафика. Так же выводятся сведения об интерфейсах, к которым применена указанная политика.

17.3.32 policy show modify-ipv6 <имя_политики> rule <номер_правила>

Вывод сведений и статистики для правила указанной политики модификации IPv6-трафика.

Синтаксис

```
policy show modify-ipv6 <имя_политики> rule <номер_правила>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики модификации IPv6-трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 65535.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения сведений и статистики для правила указанной политики модификации IPv6-трафика. Так же выводятся сведения об интерфейсах, к которым применена указанная политика.

17.3.33 policy show modify-ipv6 <имя_политики> rule <номер_правила> filter

Вывод статистики для фильтра, связанного с указанным правилом политики модификации IPv6-трафика.

Синтаксис

```
policy show modify-ipv6 <имя_политики> rule <номер_правила> filter [detail]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики модификации IPv6-трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 65535.

detail

Вывод подробных сведений.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения статистики для фильтра, связанного с указанным правилом политики модификации IPv6-трафика. Если в фильтре присутствует несколько правил, то статистика выводится по каждому правилу отдельно.

17.3.34 policy show modify-ipv6 <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>

Вывод статистики для указанного правила фильтра, связанного с указанным правилом политики модификации IPv6-трафика.

Синтаксис

```
policy show modify-ipv6 <имя_политики> rule <номер_правила> filter rule
<номер_правила_фильтра> [detail]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики модификации IPv6-трафика.

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 65535.

номер_правила_фильтра

Численный идентификатор правила фильтра. Значение должно лежать в диапазоне от 1 до 9999.

detail

Вывод подробных сведений.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения статистики для указанного правила фильтра, связанного с указанным правилом политики модификации IPv6-трафика..

18 Преобразование сетевых адресов

18.1 Обзор технологии NAT

В этом разделе описано, как настроить преобразование сетевых адресов (NAT) в системе.

В этом разделе рассматриваются следующие вопросы:

- Краткий обзор технологии NAT.
- Преимущества NAT.
- Виды NAT.
- Совместное использование NAT, маршрутизации и межсетевого экрана.

18.1.1 Краткий обзор технологии NAT

Служба преобразования сетевых адресов (NAT) - это служба, которая изменяет адрес и/или номер порта в сетевых пакетах при их прохождении через компьютер или сетевое устройство. Устройство, выполняющее преобразование сетевых адресов, может являться отправителем пакетов, получателем пакетов или промежуточным устройством на пути между отправителем и получателем.

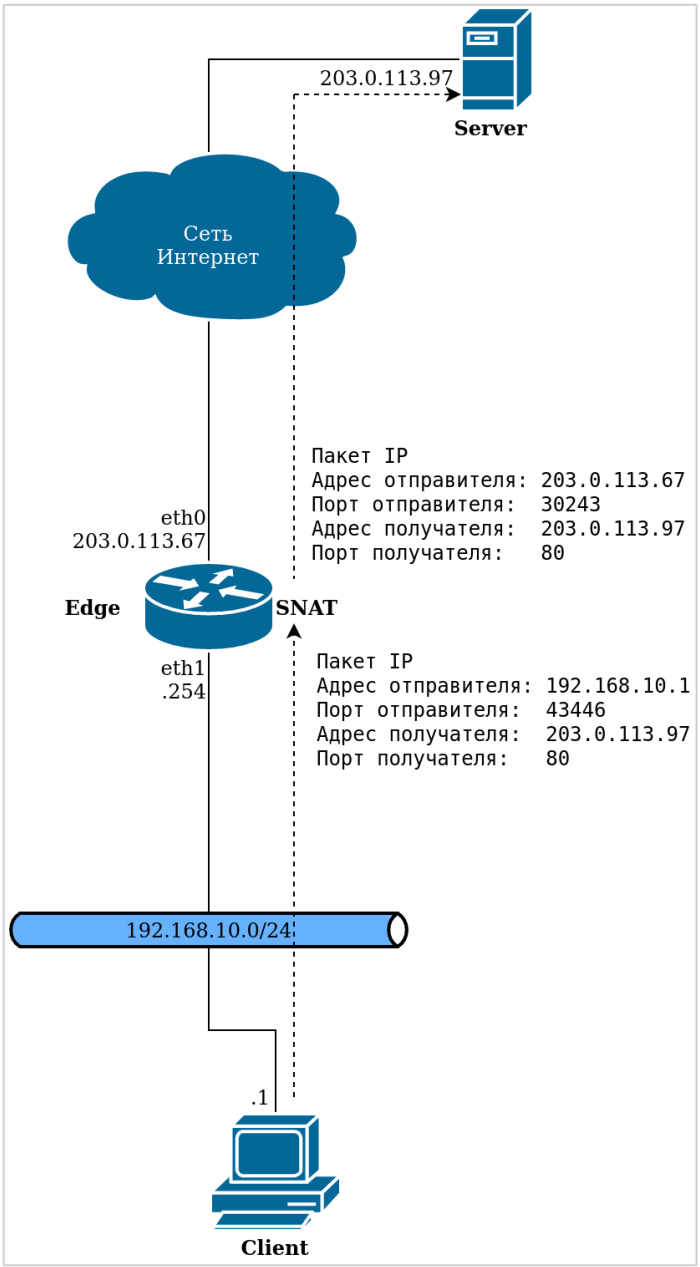


Рисунок 12 - Пример устройства, выполняющего преобразование сетевых адресов (NAT)

NAT изначально был разработан для экономии числа IP-адресов, используемых растущим числом сетевых устройств, подключенных к Интернету, однако он имеет важные применения и в безопасности сетей.

Компьютеры, расположенные во внутренней сети, могут использовать любые адреса, зарезервированные организацией IANA (Internet Assigned Numbers Authority) для частной адресации (см. также RFC 1918). Зарезервированные IP-адреса не используются в Интернете, таким образом, внешнее устройство не может осуществлять маршрутизацию на основе таких адресов. Следующие адреса зарезервированы для частного использования:

- от 10.0.0.0 до 10.255.255.255 (CIDR: 10.0.0.0/8);
- от 172.16.0.0 до 172.31.255.255 (CIDR: 172.16.0.0/12);
- от 192.168.0.0 до 192.168.255.255 (CIDR: 192.168.0.0/16);
- от 100.64.0.0 до 100.127.255.255 (CIDR: 100.64.0.0/10)

Маршрутизатор, выполняющий преобразование сетевых адресов, может скрывать IP-адреса, используемые во внутренней сети, от внешней сети посредством замены внутренних частных адресов общедоступными (public) адресами, предоставленными для этих целей. Взаимодействие с внешней сетью происходит только с использованием данных общедоступных адресов. Маршрутизатор может использовать набор общедоступных IP-адресов, из которых динамически выбирается адрес, используемый для преобразования.

Следует учитывать тот факт, что хотя использование NAT может снизить вероятность небезопасного подключения внутренних компьютеров к внешним сетям, это не обеспечивает защиты компьютеров, которые по той или иной причине подключаются к недоверенным устройствам. По этой причине всегда следует сочетать использование NAT с фильтрацией пакетов и другими возможностями политики безопасности для организации полной защиты сети.

18.1.2 Преимущества NAT

Использование преобразования сетевых адресов обеспечивает следующие преимущества:

- NAT позволяет более эффективно использовать глобальное адресное пространство Интернета.
  Любое число устройств локальной сети может использовать частные IP-адреса вместо использования общедоступных IP-адресов. Адреса пакетов, передаваемых из внутренней сети во внешнюю, преобразуются в предназначенные для этого общедоступные IP-адреса. Это означает, что одно и то же частное адресное пространство может быть использовано неограниченным количеством частных сетей, как представлено на рисунке.

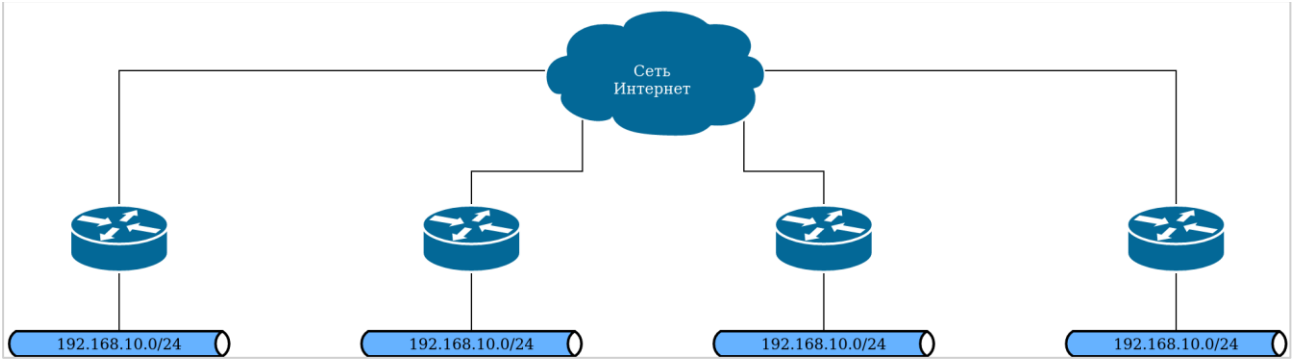


Рисунок 13 – Повторное использование адресного пространства

- NAT позволяет повысить уровень безопасности.
- IP-адреса, используемые в частных (внутренних) сетях, скрыты от сетей общего пользования (внешних). Это осложняет проведение злоумышленником атаки на узел внутренней сети. Однако узлы частной сети по прежнему остаются уязвимыми, и по этой причине NAT обычно используется совместно с межсетевым экранированием.

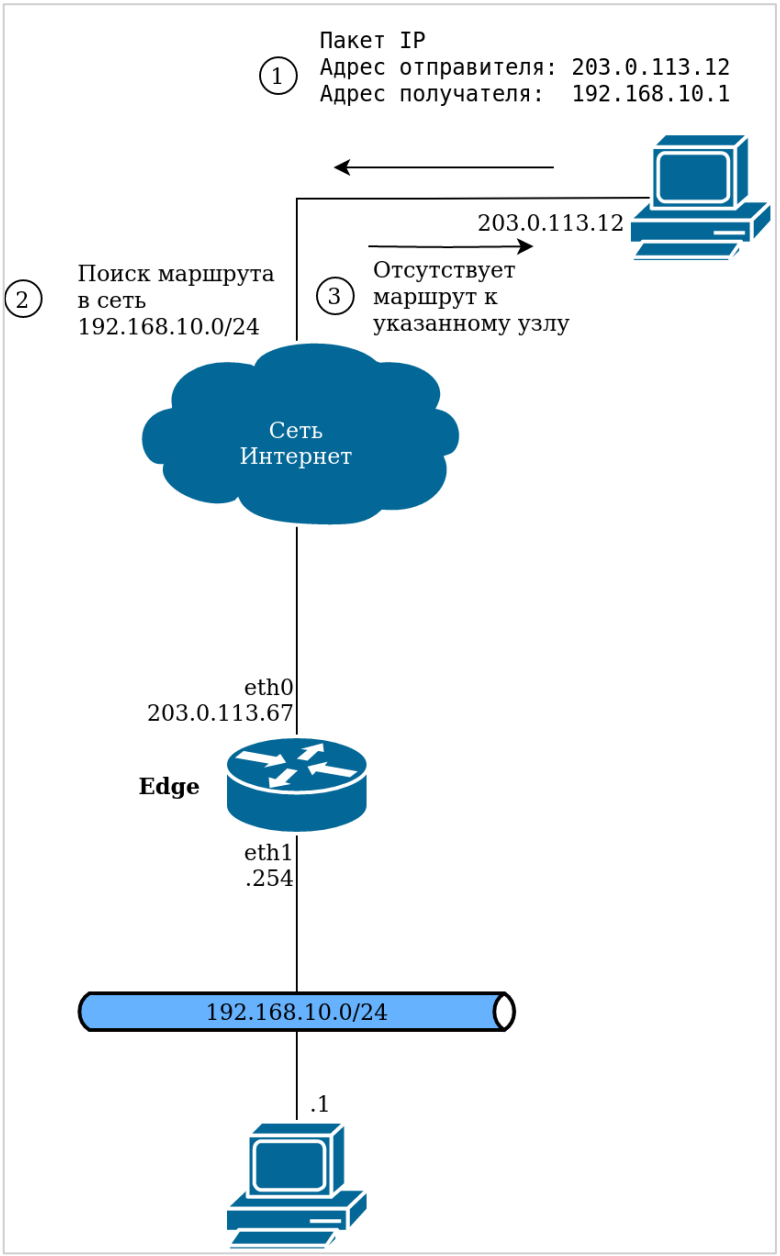


Рисунок 14 – Совместное использование NAT и межсетевого экрана

- Стандартные клиент-серверные сетевые службы не требуют модификации при функционировании поверх устройств, осуществляющих преобразование сетевых адресов.
- Технология NAT облегчает перемещение из одного адресного пространства в другое.
  Адресное пространство, используемое внутри частной сети, расположенной за NAT, не зависит от внешнего IP-адреса. Это означает, что для частной сети может быть изменен внешний IP-адрес без дополнительного изменения сетевых настроек внутри частной сети. Аналогично этому, изменение внутренней адресации частной сети не повлияет на внешний IP-адрес.
- Использование NAT упрощает маршрутизацию.
  Технология NAT избавляет от необходимости использования сложных схем маршрутизации в больших сетях.

18.1.3 Виды NAT

Существует три основных вида преобразования сетевых адресов (NAT):

- Преобразование сетевого адреса отправителя (SNAT).
- Преобразование сетевого адреса получателя (DNAT).
- Двунаправленное преобразование сетевых адресов (SNAT + DNAT).

Преобразование сетевого адреса отправителя (SNAT)

ПРИМЕЧАНИЕ SNAT выполняется после маршрутизации

SNAT представляет собой наиболее часто используемый вид NAT. SNAT изменяет адрес отправителя сетевых пакетов, проходящих через систему. SNAT обычно используется в том случае, когда внутреннему узлу необходимо инициировать сеанс связи с общедоступным узлом; в этом случае устройство, выполняющее преобразование адресов, изменяет частный IP-адрес узла отправителя на некоторый общедоступный IP-адрес, как представлено на рисунке ниже. При использовании "маскировки" (частный случай SNAT) адрес отправителя исходящего пакета заменяется основным IP-адресом выходного интерфейса. Устройство, выполняющее преобразование пакетов, отслеживает информацию о потоке сетевого трафика таким образом, чтобы сетевой трафик корректно пересылался к отправителю и от него.

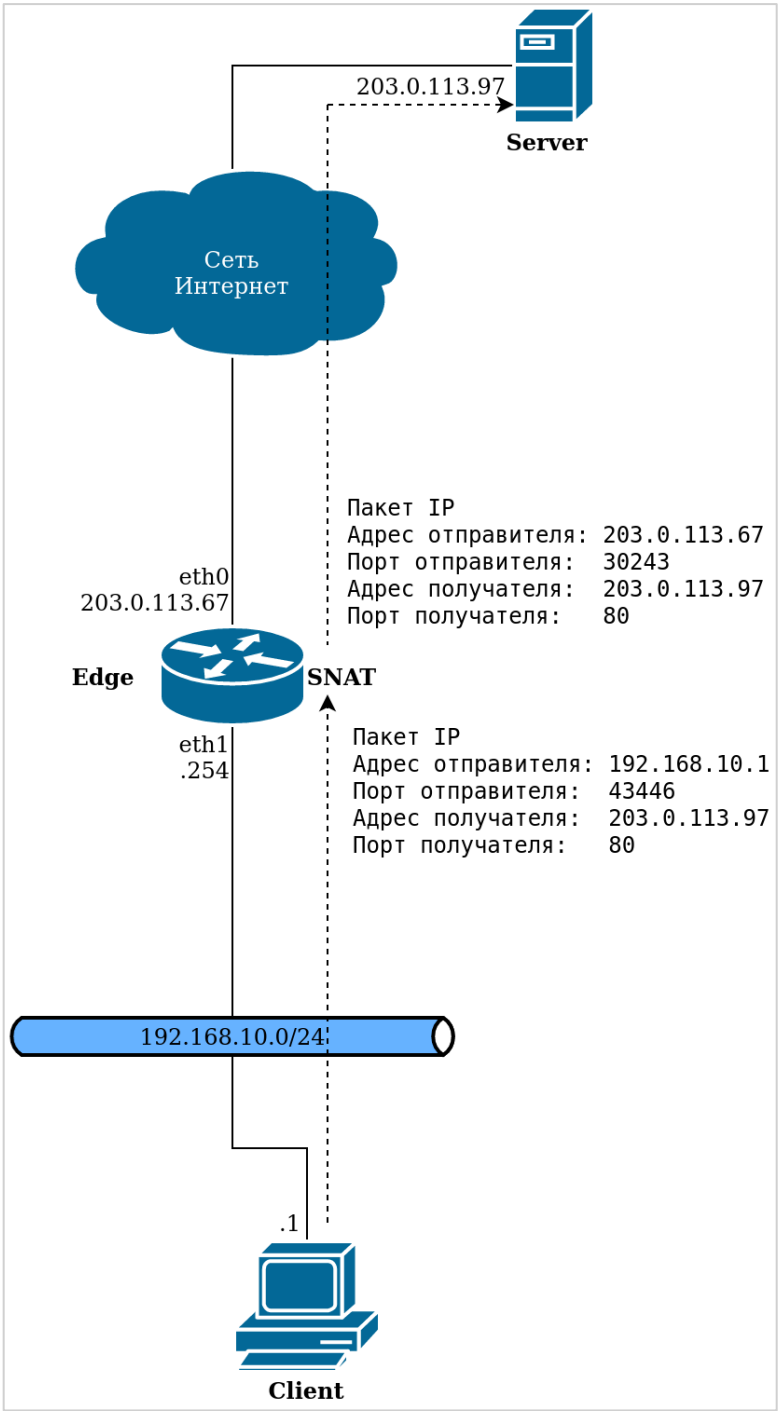


Рисунок 14 – Преобразование сетевого адреса отправителя (SNAT)

Преобразование сетевого адреса получателя (DNAT)

ПРИМЕЧАНИЕ DNAT выполняется перед маршрутизацией

В то время как SNAT изменяет адрес отправителя сетевых пакетов, DNAT изменяет адрес получателя сетевых пакетов при их прохождении через систему. DNAT обычно используется в тех случаях, когда общедоступному узлу требуется инициировать сеанс связи со внутренним (частным) узлом; например, когда подписчик получает доступ к новостному серверу, как представлено на рисунке.

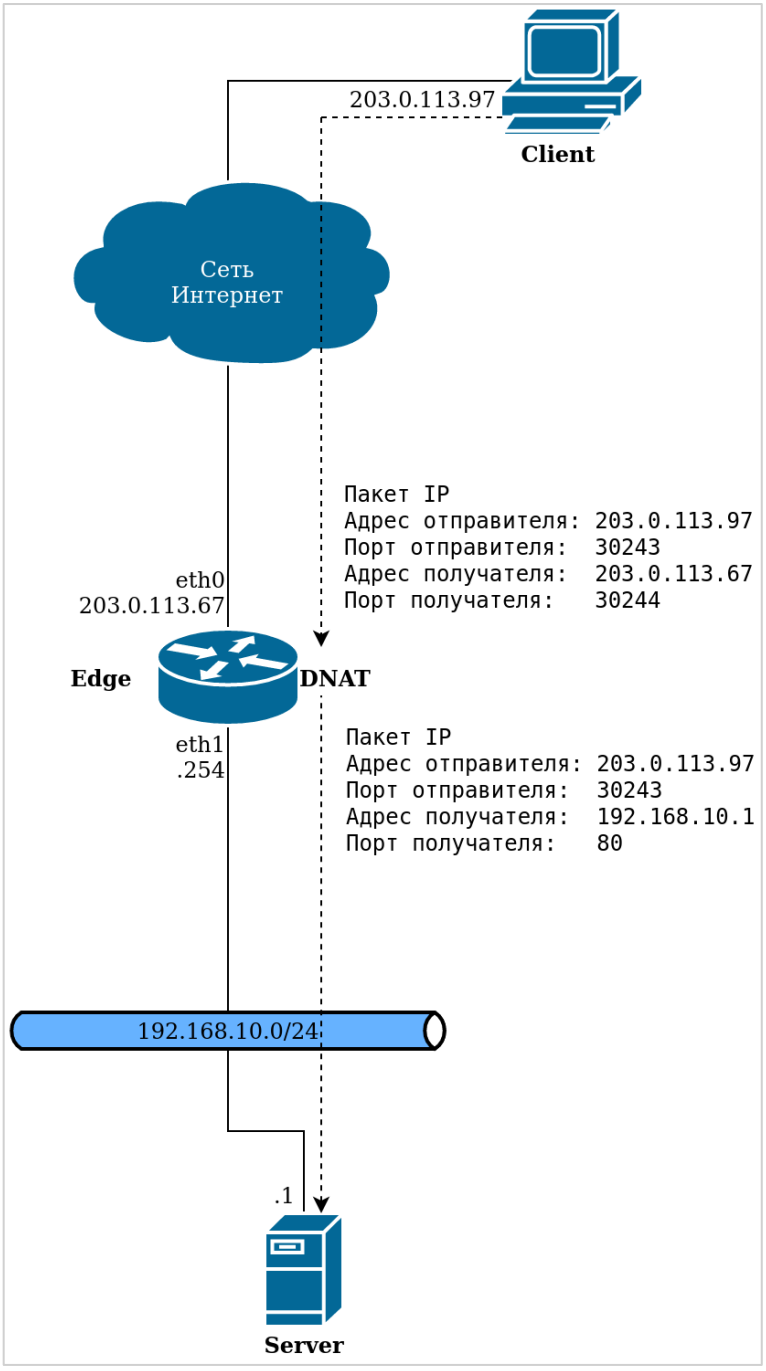


Рисунок 15 – Преобразование сетевых адресов получателя (DNAT)

Двунаправленное преобразование сетевых адресов (SNAT + DNAT)

Двунаправленное преобразование сетевых адресов представляет собой схему, в которой одновременно используется как SNAT, так и DNAT. Двунаправленное преобразование сетевых адресов обычно используется, когда внутренним узлам требуется инициировать сеансы связи со внешними узлами, а также внешним узлам требуется инициировать сеансы связи со внутренними узлами. На рисунке приведен пример двунаправленного NAT.

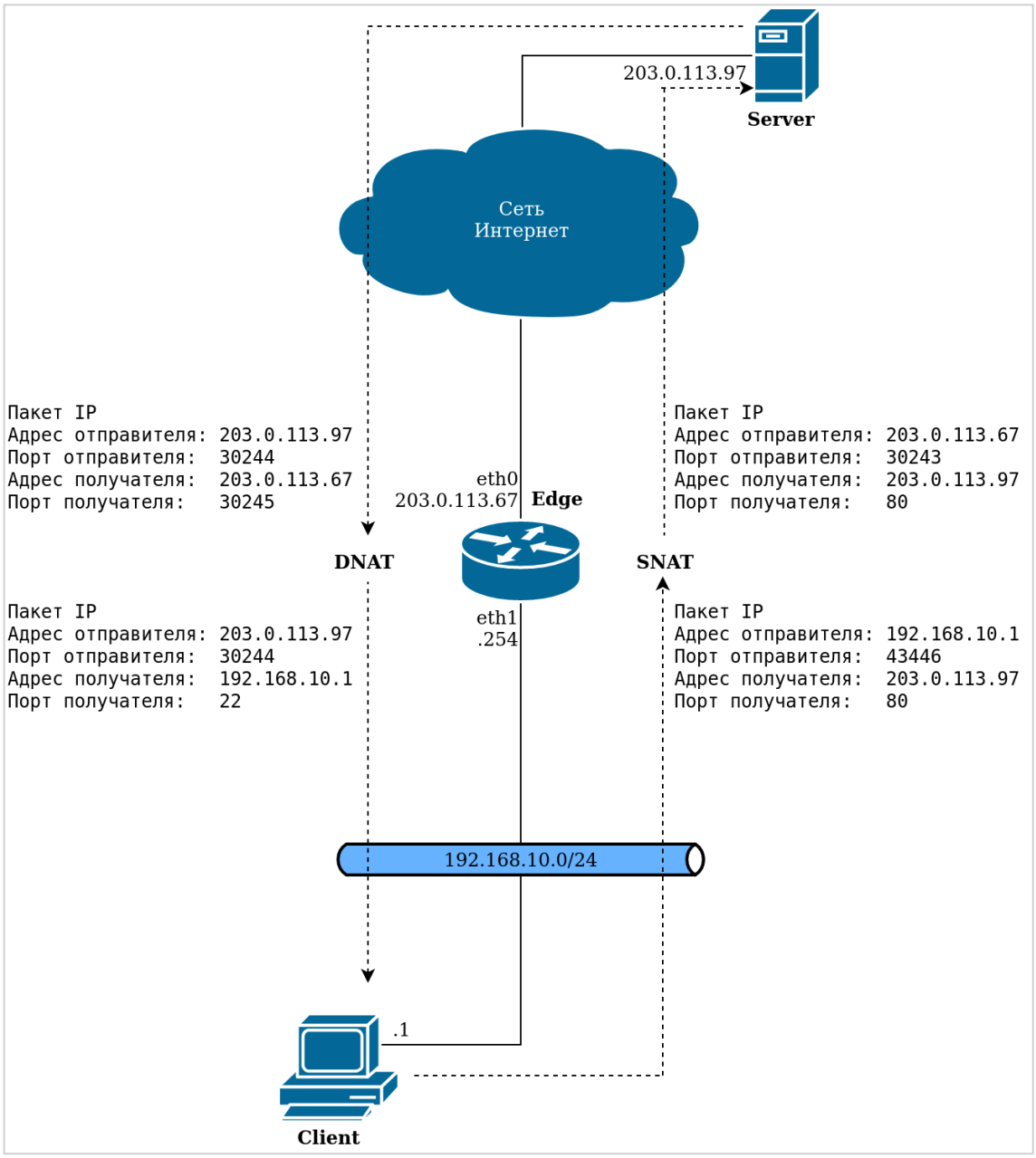


Рисунок 16 – Двунаправленное преобразование сетевых адресов

18.1.4 Совместное использование NAT, маршрутизации и межсетевого экрана

Одним из наиболее важных моментов, о котором необходимо иметь представление при использовании преобразования сетевых адресов, является порядок обработки пакетов различными службами, настроенными в системе. Если порядок обработки не учитывается, могут быть получены результаты, отличные от ожидаемых.

Например, при использовании DNAT необходимо следить за тем, чтобы маршрутизация была настроена не на основе конкретных внешних адресов. Это может привести к непредсказуемым результатам, так как адреса внешних пакетов будут заменены на внутренние адреса механизмом преобразования сетевых адресов получателя (DNAT) перед выполнением маршрутизации.

Также использование технлологии NAT оказывает влияние на работу определенных фильтров трафика, которые могут использоваться в политиках межсетевого экранирования. Так, например, фильтрация по фрагментированным пакетам и фильтрация по некорректным флагам для протокола TCP не работают совместно с NAT ввиду особенностей реализации сохранения соединений в таблицу.

На рисунке представлена схема прохождения трафика при использовании NAT, маршрутизации и межсетевого экрана.

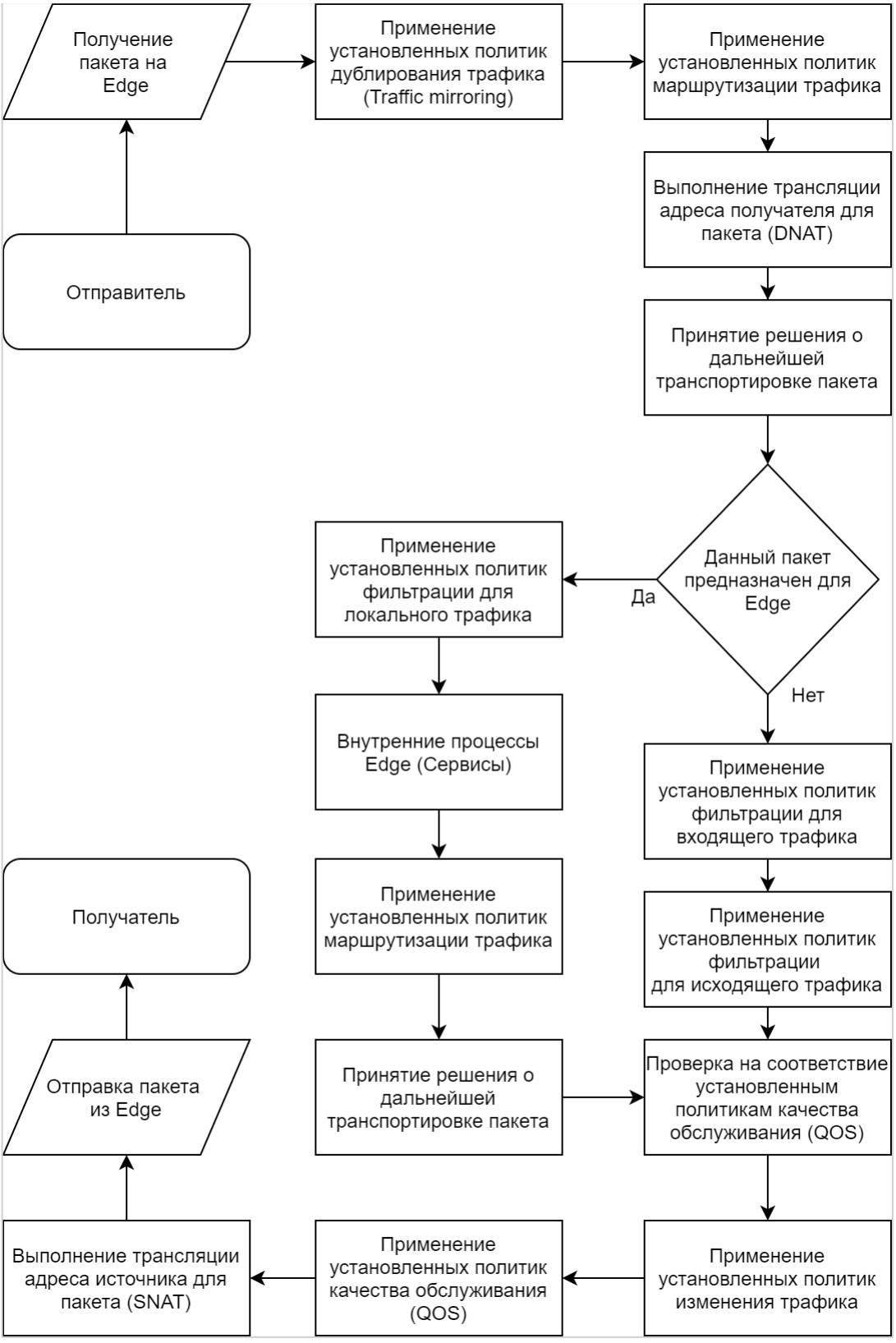


Рисунок 17 – Прохождение трафика через Numa Edge

На рисунке 18 изображена базовая схема сети, которая будет использоваться в дальнейших примерах.

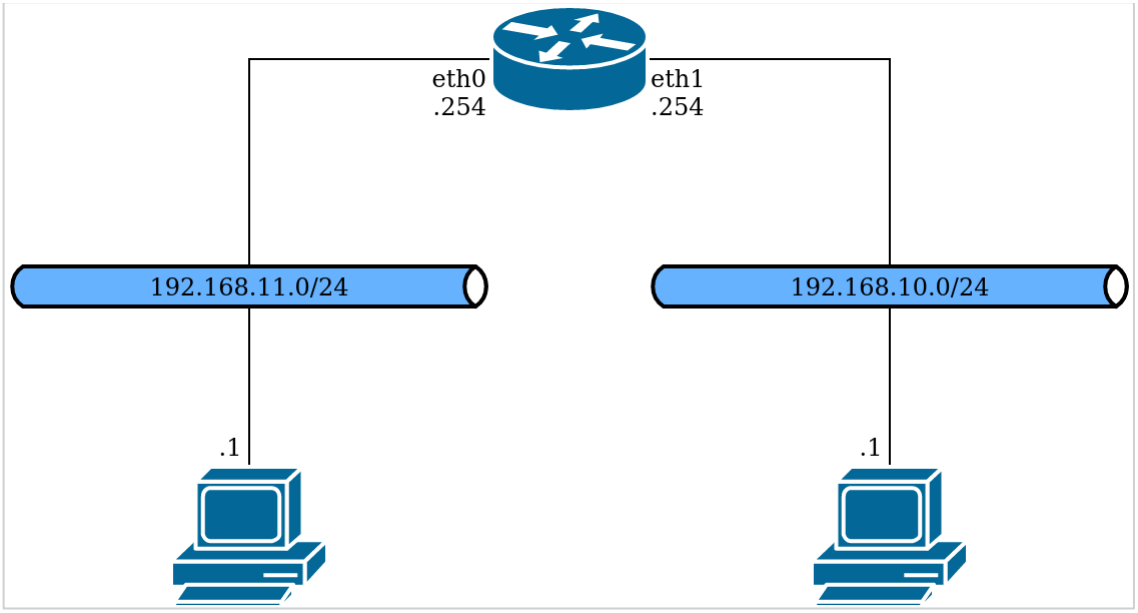


Рисунок 18 - Базовая схема

Совместное использование NAT и маршрутизации

При совместном использовании NAT и маршрутизации необходимо учитывать влияние правил DNAT и SNAT на решения о маршрутизации. Типовые схемы, приведенные в этом разделе, раскрывают данный вопрос.

- Схема 1a. DNAT — Пакеты, проходящие через Numa Edge
- Схема 1б. DNAT — Пакеты, предназначенные для Numa Edge
- Схема 2a. SNAT — Пакеты, проходящие через Numa Edge
- Схема 2б. SNAT — Пакеты, отправителем которых является Numa Edge

Схема 1a. DNAT—Пакеты, проходящие через Numa Edge

ПРИМЕЧАНИЕ DNAT — решение о маршрутизации принимается на основе измененных адресов получателя

Преобразование DNAT осуществляется перед принятием решения о маршрутизации. Это означает, что принятие решения о маршрутизации на основе адреса получателя осуществляется с использованием измененных адресов получателя — а не первоначальных адресов получателя;

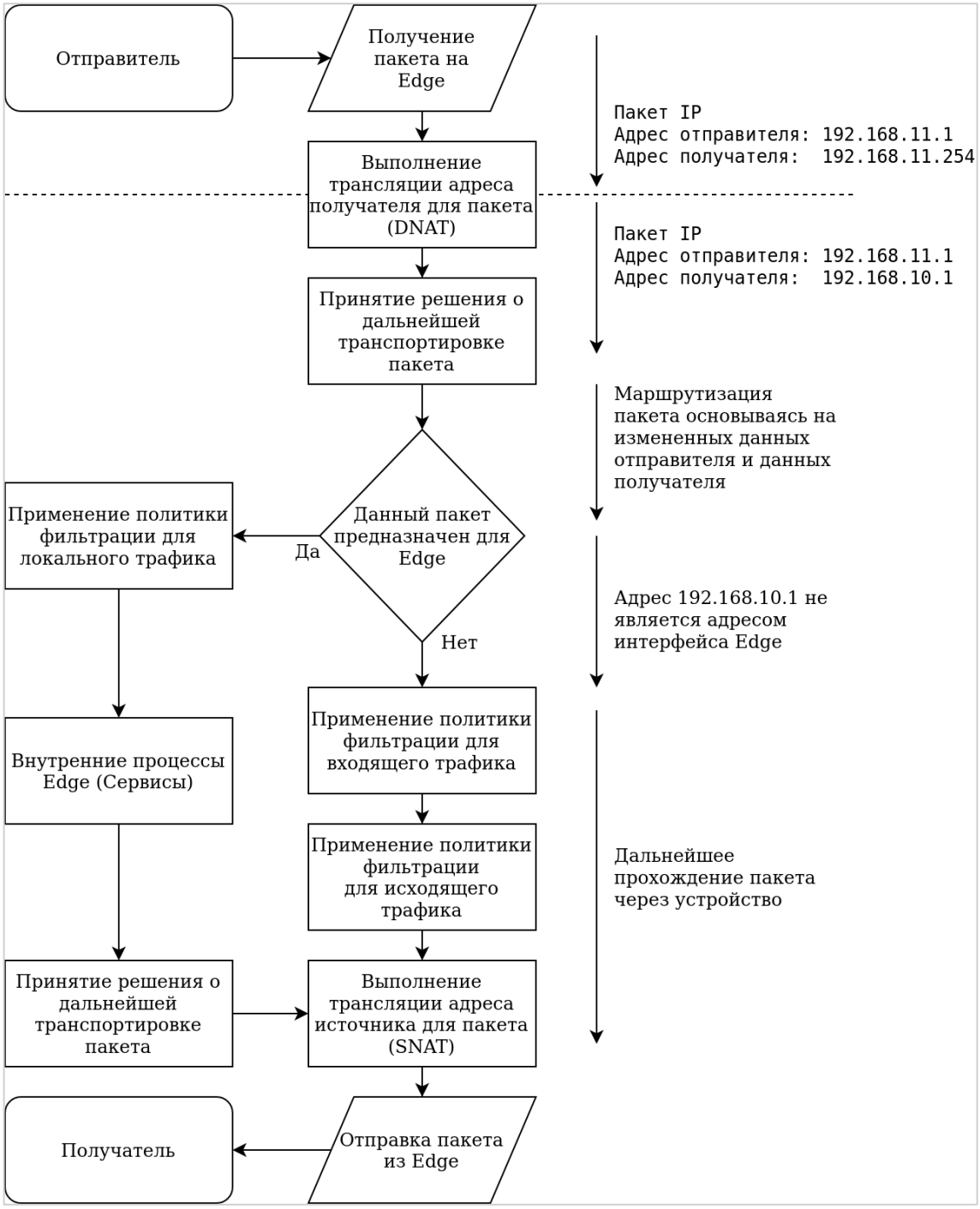


Рисунок 19 – Решения о маршрутизации при прохождении DNAT

Схема 1б. DNAT— Пакеты, предназначенные для Numa Edge

Аналогичная ситуация происходит, когда сетевые пакеты предназначаются для локальной системы. В этой схеме пакеты предназначены для одного из локальных процессов системы.

Опять же, так как преобразование DNAT применяется к сетевым пакетам перед принятием решения о маршрутизации, принятие решения о маршрутизации осуществляется на основе измененных адресов получателя — а не первоначальных адресов.

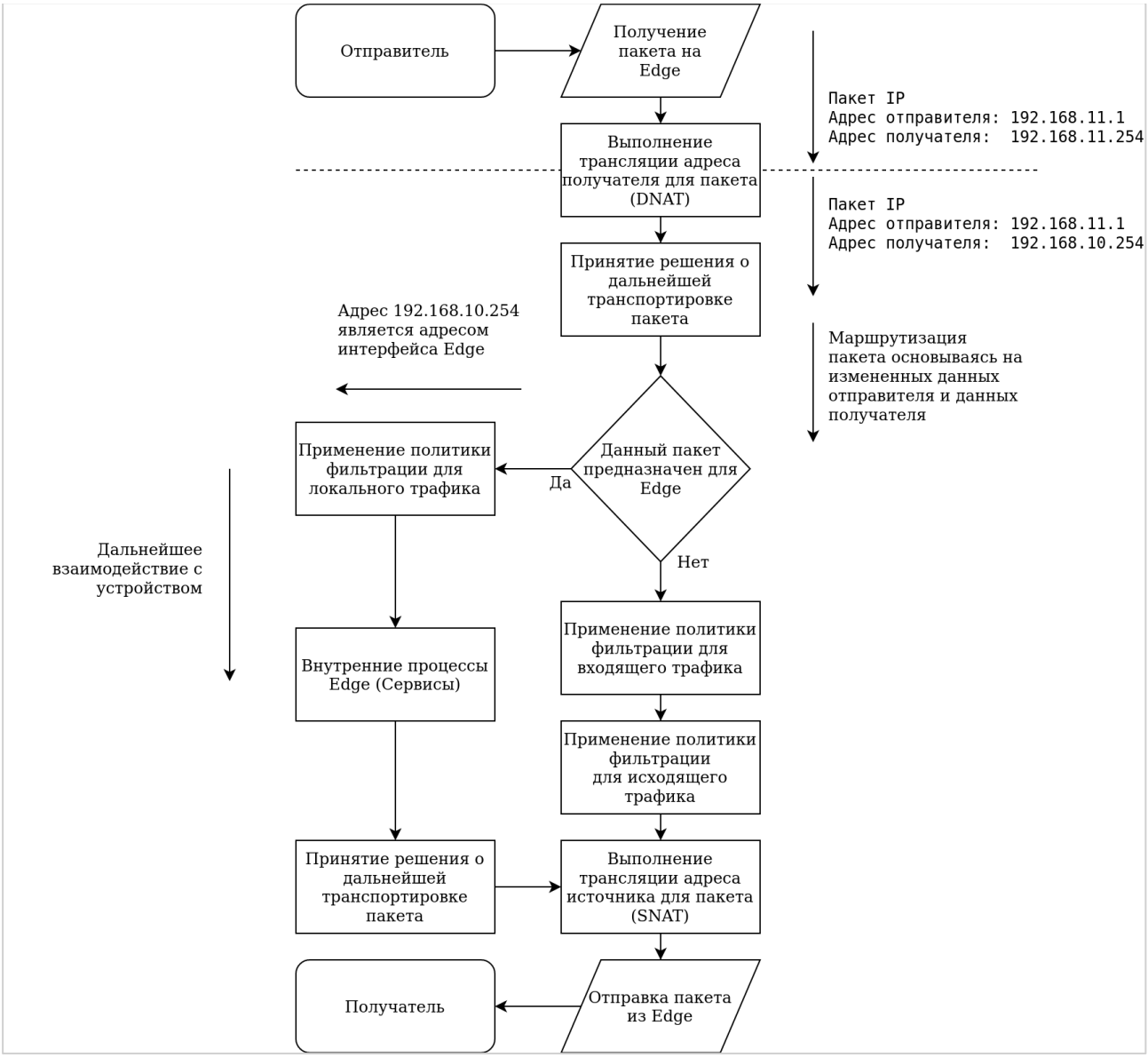


Рисунок 20 – Решения о маршрутизации при использовании DNAT для пакетов, предназначенных Numa Edge

Схема 2a. SNAT— Пакеты, проходящие через Numa Edge

ПРИМЕЧАНИЕ SNAT — Решение о маршрутизации принимается на основе исходного (первоначального) адреса отправителя

В то же время решения о маршрутизации принимаются *перед* преобразованием SNAT. Это означает, что принятие решения о маршрутизации на основе адресов отправителя осуществляется на основе *исходного (первоначального)* адреса отправителя — а *не* измененного адреса;

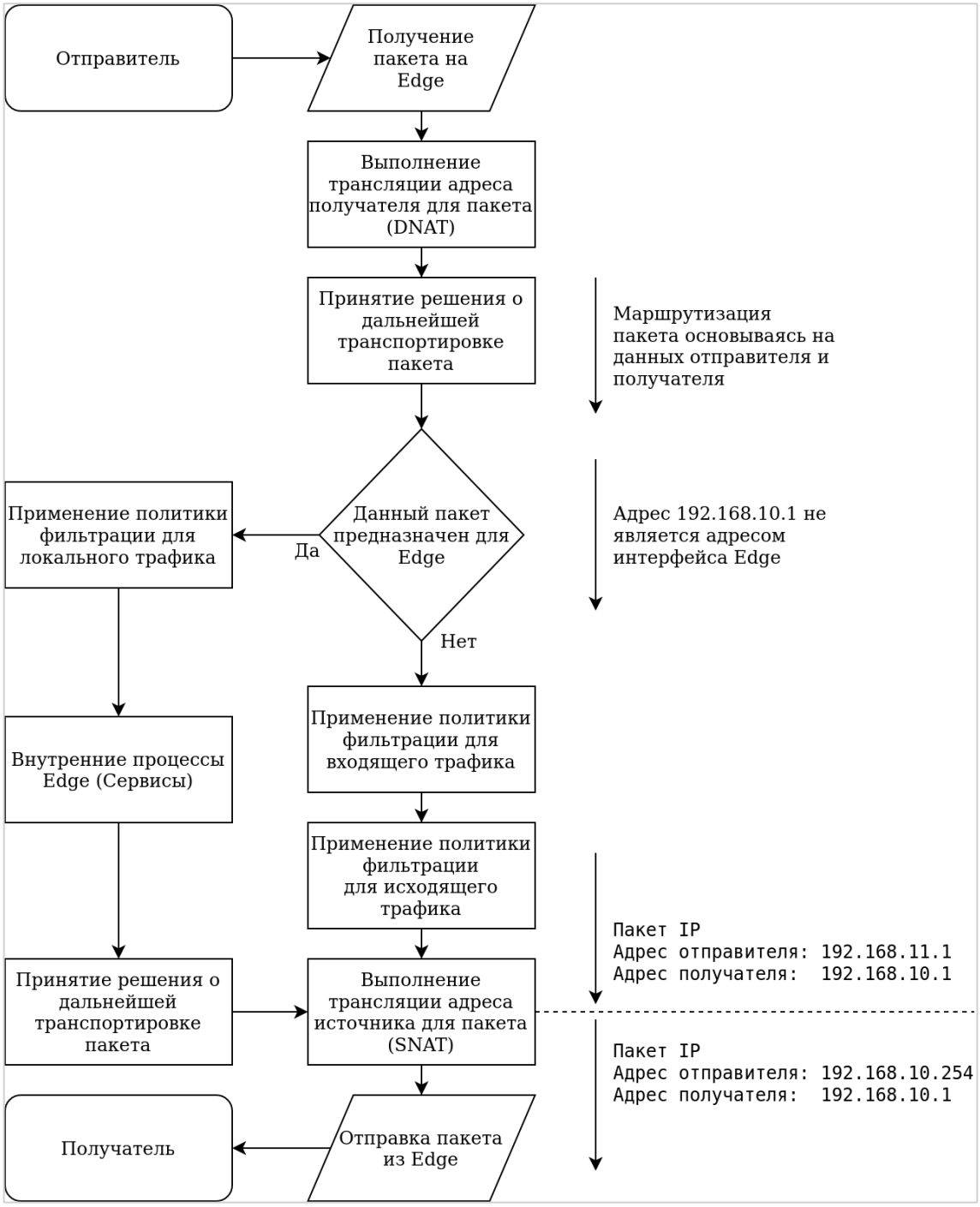


Рисунок 21 - Решения о маршрутизации при прохождении SNAT

Схема 26. SNAT— Пакеты, отправителем которых является Numa Edge

В этой схеме сетевые пакеты отправляются процессом внутри Numa Edge.

В свою очередь, так как принятие решения о маршрутизации осуществляется перед преобразованием сетевого адреса отправителя, принятие решения о маршрутизации на основе адреса отправителя осуществляется с использованием исходного (первоначального) адреса отправителя — а не измененного адреса.

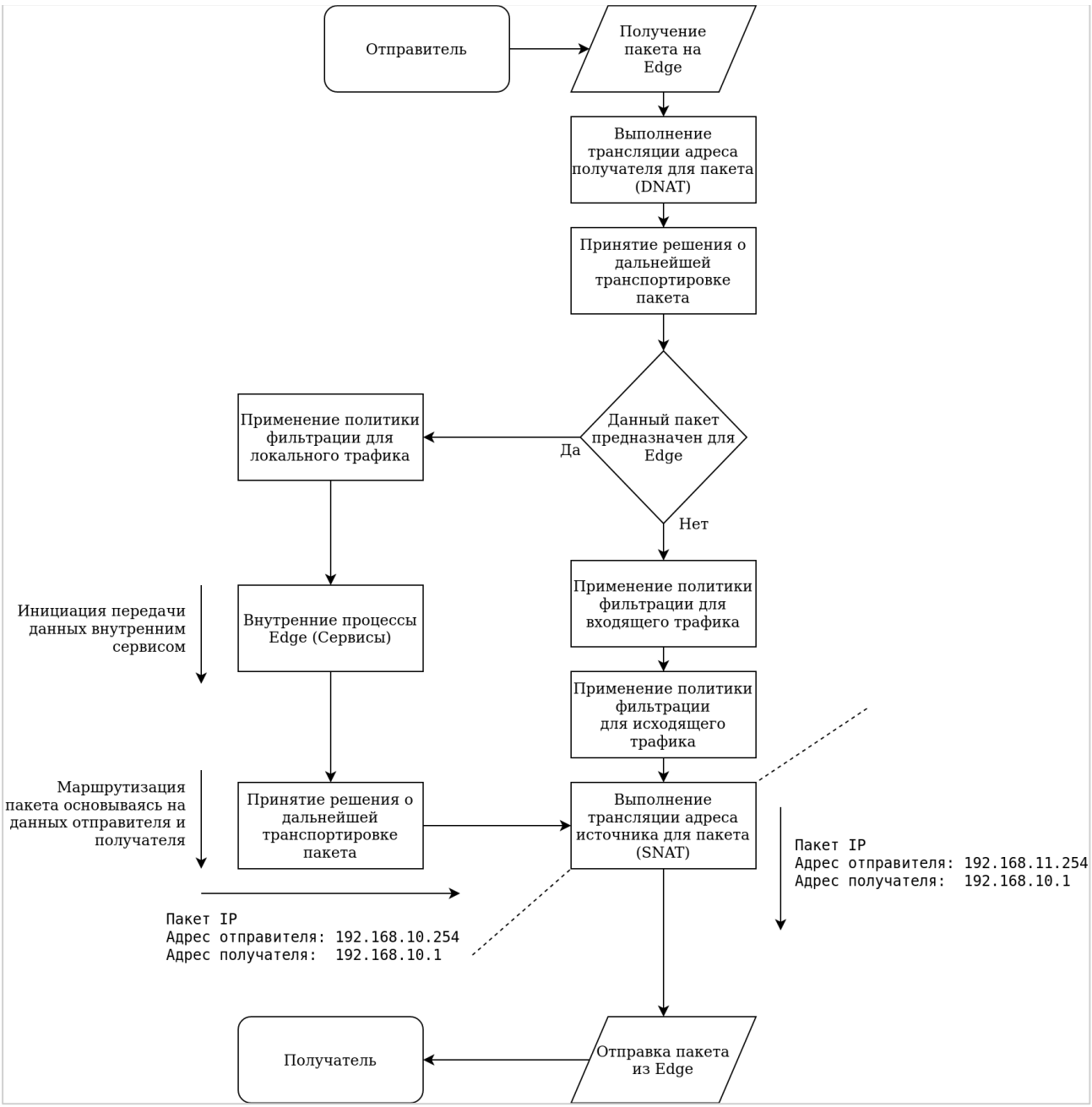


Рисунок 22 – Решения о маршрутизации при использовании SNAT для пакетов, отправленных Numa Edge

Совместное использование NAT и межсетевого экранирования

При совместном использовании NAT и межсетевого экрана важно иметь представление о последовательности обработки сетевого трафика данными службами. Типовые схемы, приведенные в этом разделе, раскрывают этот вопрос:

- Схема 3а. DNAT—Пакеты, проходящие через Numa Edge
- Схема 3б. DNAT— Пакеты, предназначенные для Numa Edge
- Схема 4а. SNAT— Пакеты, проходящие через Numa Edge
- Схема 4б. SNAT— Пакеты, отправителем которых является Numa Edge

Схема 3а. DNAT—Пакеты, проходящие через Numa Edge

В этой схеме сетевые пакеты отправлены из сети A и проходят через Numa Edge.

Правила межсетевого экрана, установленные для входящего трафика, применяются после осуществления преобразования сетевого адреса получателя (то есть на основе измененного адреса получателя).

Правила межсетевого экрана, установленные для исходящего трафика, применяются после осуществления преобразования сетевого адреса получателя (то есть, на основе измененного адреса получателя);

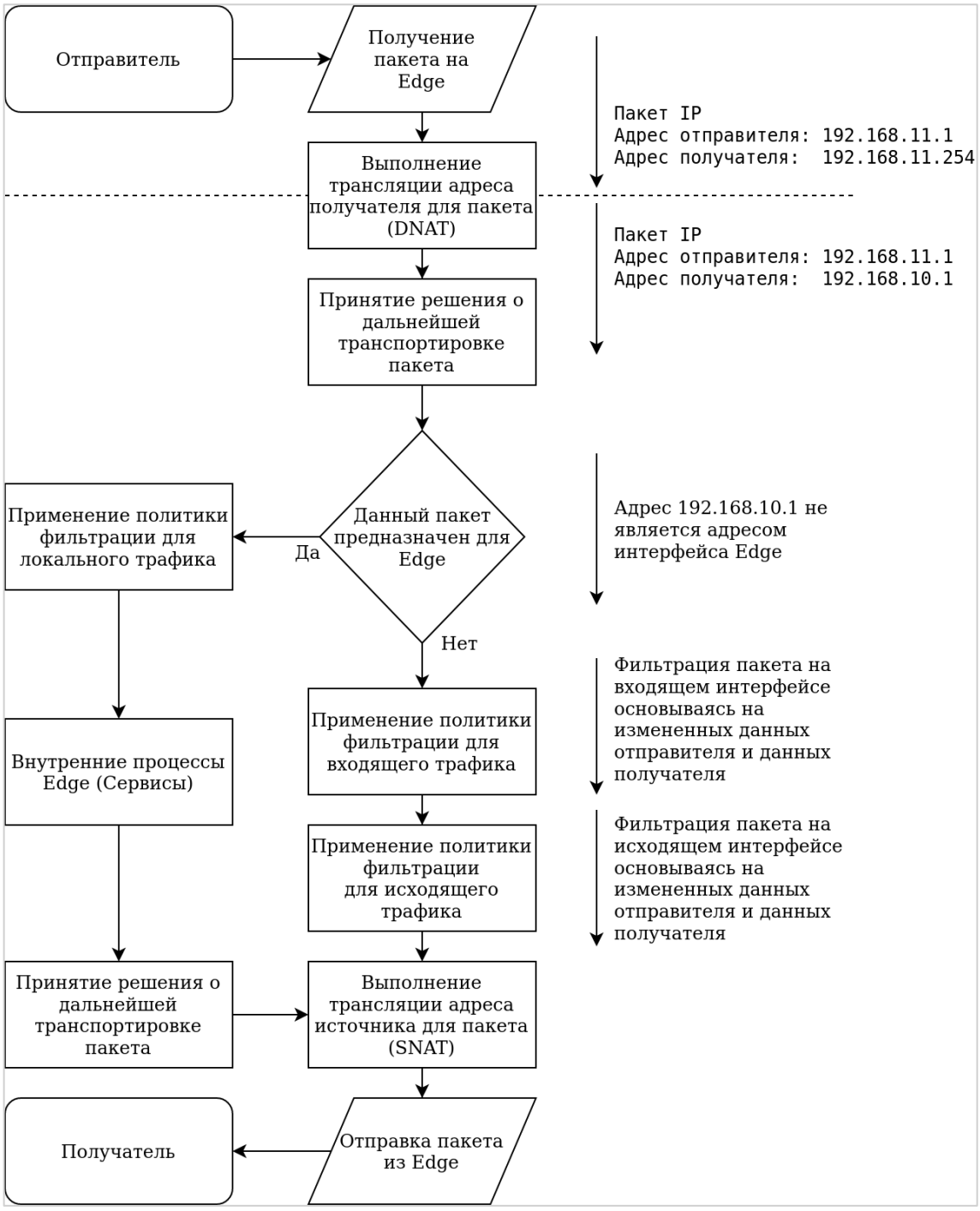


Рисунок 23 – Решение МЭ при прохождении DNAT

Схема 36. DNAT— Пакеты, предназначенные для Numa Edge

В этой схеме пакеты предназначены для одного из процессов в Numa Edge. Правила межсетевого экрана, установленные для трафика предназначенного для локальной системы, применяются после осуществления преобразования сетевого адреса получателя (то есть, на основе измененного адреса получателя)

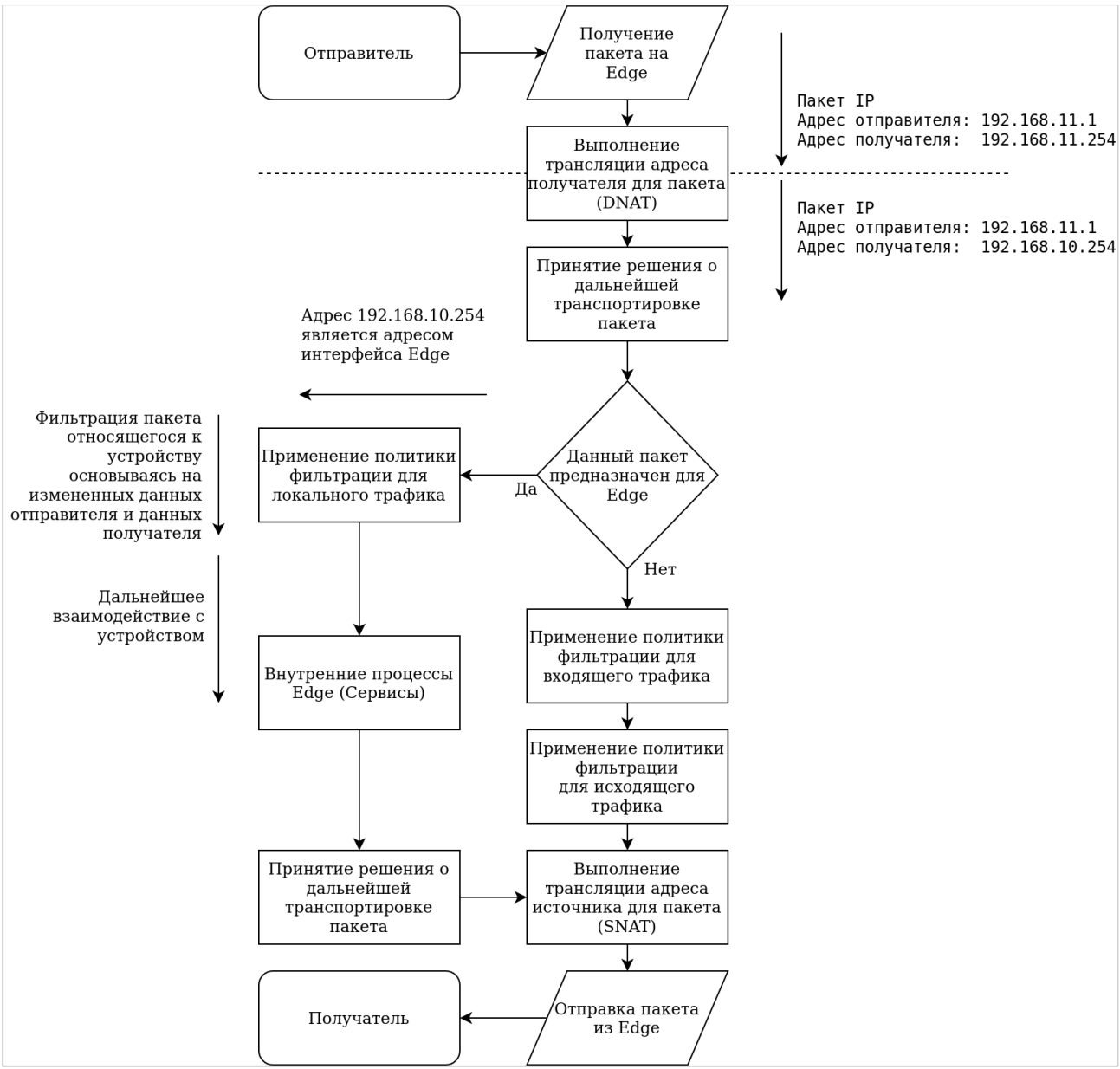


Рисунок 24 – Решения МЭ при использовании DNAT для пакетов, предназначенных Numa Edge

Схема 4a. SNAT— Пакеты, проходящие через Numa Edge

ПРИМЕЧАНИЕ Правила SNAT осуществляются на основе исходного (первоначального) адреса отправителя.

Правила межсетевого экрана, установленные для входящего и исходящего трафика, применяются до осуществления преобразования сетевого адреса отправителя. Это означает, что решения МЭ принимаются на основе исходного (первоначального) адреса отправителя — а не измененного адреса отправителя.

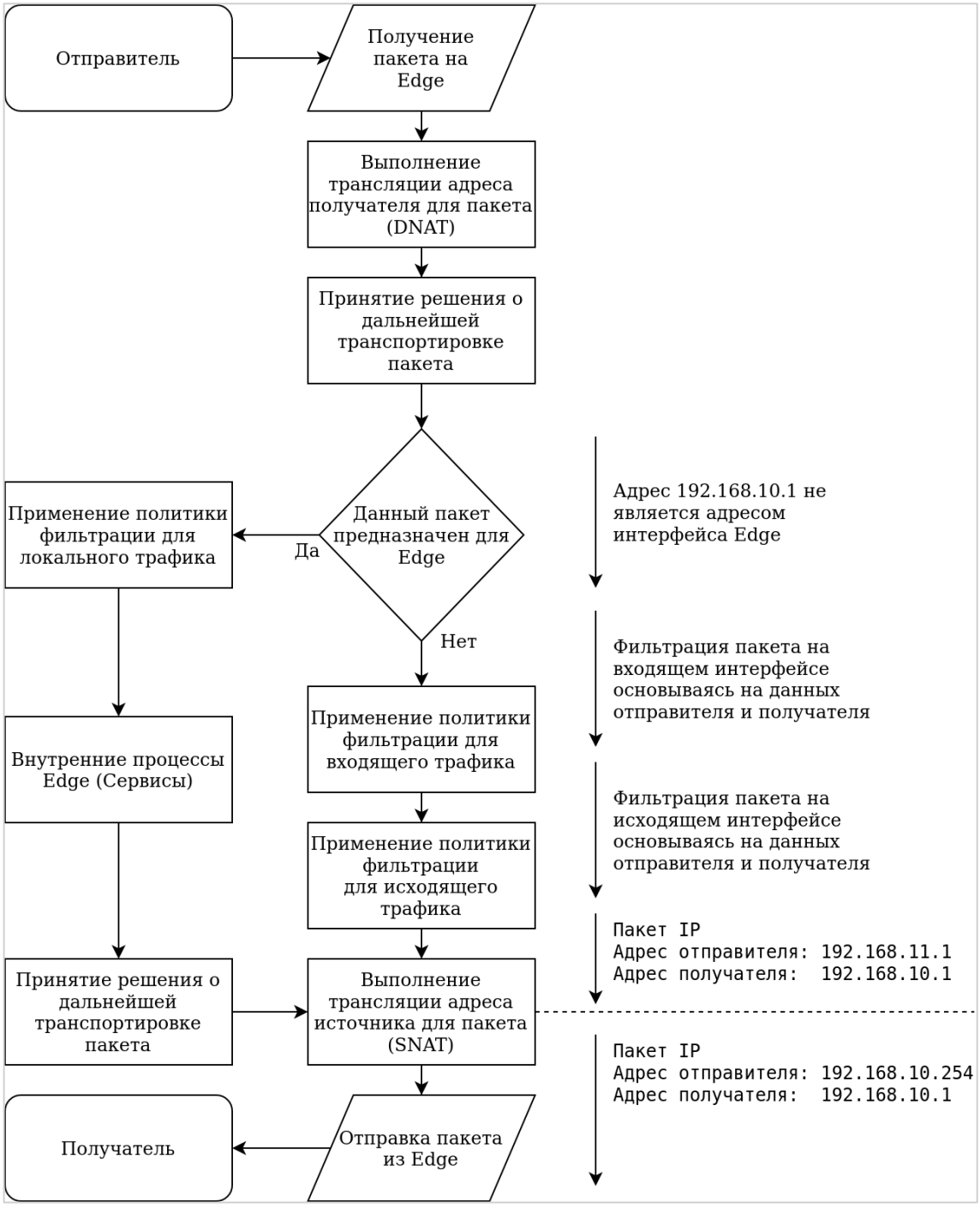


Рисунок 25 – Решения МЭ при использовании SNAT для пакетов, проходящих через Numa Edge

Схема 46. SNAT— Пакеты, отправителем которых является Numa Edge

В данной схеме сетевые пакеты отправляются одним из процессов в Numa Edge. Правила установленные для исходящих пакетов применяются применяются к исходному (первоначальному) адресу отправителя, а не измененному адресу.

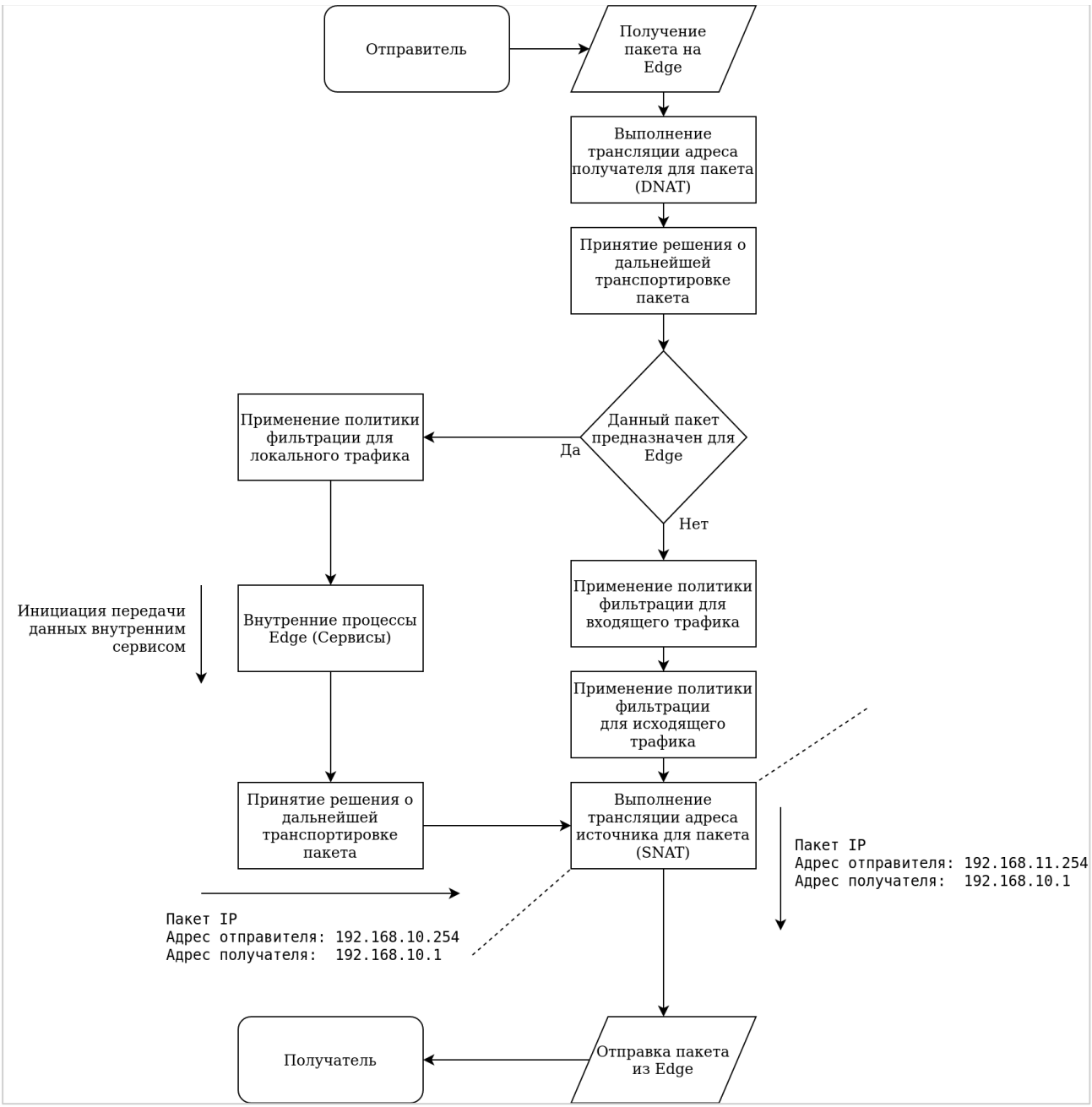


Рисунок 26 – Решения МЭ при использовании SNAT для пакетов, отправленных Numa Edge

18.2 Структура создания правила NAT

NAT настраивается в качестве набора правил. Каждое правило предписывает NAT осуществить требуемое преобразование адресов. Правила NAT нумеруются и исполняются в соответствующем порядке.

Следует учесть, что в настроенном правиле NAT номер является неизменяемым идентификатором. Номер правила NAT не может быть изменен так же, как, например, изменяются атрибуты правила. Для изменения номера правила NAT следует удалить правило и создать его заново с новым номером. Так же можно воспользоваться командами **copy** и **rename**, позволяющими копировать и переименовывать имена соответствующих узлов конфигурации.

ПРИМЕЧАНИЕ Следует оставлять интервалы между номерами правил NAT

По этой причине следует назначать правилам NAT номера, оставляя пустые интервалы между номерами. Например, можно создать набор правил NAT с номерами 10, 20, 30 и 40. Таким образом, если позже потребуется добавить еще одно правило для выполнения в конкретном месте в последовательности правил, это будет легко сделать без удаления текущего набора правил.

Схема, использующаяся в примерах, представлена ниже

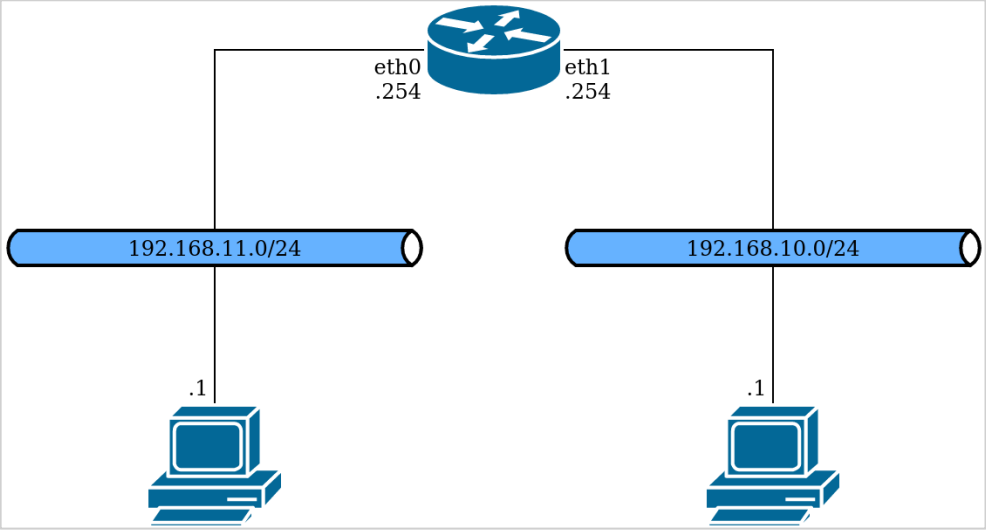


Таблица 131 – Схема настройки

- Узел конфигурации
- Настройка типа NAT
- Настройка критериев фильтрации трафика
- Настройка адресов преобразования
- Настройка интерфейсов
- Итоговая конфигурация

18.2.1 Узел конфигурации

Для создания или изменения правила NAT используются команды set и узел конфигурации service nat ipv4 с указанием номера, который будет являться идентификатором правила; см. пример ниже:

Пример 135 – Создание правила NAT

```
admin@edge# set service nat ipv4 rule 10
```

18.2.2 Настройка типа NAT

Существует возможность создания правил преобразования сетевых адресов отправителя, преобразования сетевых адресов получателя и правил маскировки (типы: source (SNAT), destination (DNAT) или masquerade ("маскировка")). Для осуществления двунаправленного преобразования сетевых адресов следует определить два правила: одно для SNAT и одно для DNAT. В примере 136 определяется правило SNAT с номером 10.

Пример 136 – Создание правила преобразования сетевого адреса отправителя (SNAT)

```
admin@edge# set service nat ipv4 rule 10 type source
admin@edge# set service nat ipv4 rule 15 type destination
```

18.2.3 Настройка критериев фильтрации трафика

Фильтры позволяют контролировать, к каким пакетам следует применять правила преобразования сетевых адресов. Для правила NAT могут быть созданы фильтры трех видов: на основе протоколов (**protocols**), на основе адреса отправителя (**source**), а также на основе адреса получателя (**destination**).

Фильтр на основе протоколов

Параметр **protocols** позволяет указать сетевые протоколы, к пакетам которых следует применять правила преобразования сетевых адресов. Таким образом, адреса будут изменяться только для пакетов указанных протоколов. По умолчанию определены все (**all**) протоколы.

В примере ниже настраивается применение правила 15 к пакетам протокола TCP. Преобразование сетевых адресов будет осуществляться только для пакетов протокола TCP.

Пример 137 – Фильтрация пакетов на основе протоколов

```
admin@edge# set service nat ipv4 rule 15 protocol tcp
```

Фильтр на основе данных отправителя

Параметр **source** позволяет фильтровать пакеты на основе адреса отправителя и/или номера сетевого порта. Преобразование сетевых адресов будет применяться только к сетевым пакетам, адрес отправителя и/или номер сетевого порта которых совпадает с указанным. (Указание номера сетевого порта является необязательным.)

Если фильтр на основе адреса отправителя не определен, по умолчанию преобразование сетевых адресов применяется к пакетам с любым адресом отправителя и/или номером сетевого порта.

В примере ниже настраивается применение правила 10 только к пакетам, адрес отправителя которых равен 192.168.11.1.

Пример 138 – Фильтрация на основе адреса отправителя

```
admin@edge# set service nat ipv4 rule 10 source address 192.168.11.1
```

В примере ниже настраивается применение правила 15 к пакетам, адрес отправителя которых принадлежит сети 192.168.11.0/24, а номер сетевого порта отправителя равен 80.

Пример 139 – Фильтрация на основе сети отправителя и номера сетевого порта

```
admin@edge# set service nat ipv4 rule 15 source address 192.168.11.0/24
admin@edge# set service nat ipv4 rule 15 source port 80
```

Фильтр на основе адреса получателя

Параметр **destination** позволяет фильтровать пакеты на основе адреса и/или номера сетевого порта получателя. Преобразование сетевых адресов будет применяться только к сетевым пакетам, адрес и номер сетевого порта получателя которых совпадает с указанным. (Указание номера сетевого порта является необязательным.)

Если фильтрация на основе адреса получателя не определена, по умолчанию преобразование сетевых адресов применяется к пакетам с любым адресом и номером сетевого порта получателя.

В примере ниже настраивается применение правила 10 к пакетам, адрес получателя которых равен 192.168.11.254.

Пример 140 – Фильтрация на основе адреса получателя

```
admin@edge# set service nat ipv4 rule 10 destination address 192.168.11.254
```

Фильтрация может выполняться не только на основе адреса получателя, но и на основе его номера порта.

18.2.4 Настройка адресов преобразования

Параметры **inside-address** и **outside-address** позволяют определить вид преобразования, которое будет осуществляться в правиле. Они определяют данные, используемые для замены исходных адресов сетевых пакетов.

Внутренний адрес

Параметр **inside-address** используется для настройки преобразования сетевого адреса получателя (DNAT). Позволяет определить адрес, который будет использоваться для замены IP-адреса получателя входящего сетевого пакета. Также может использоваться преобразование номеров портов (port translation), в этом случае номер сетевого порта указывается как часть определяемого внутреннего адреса.

В примере ниже настраивается применение правила 20, которое будет подставлять адрес 192.168.10.1 в качестве IP-адреса входящего пакета для пакетов, удовлетворяющих условиям, определенным в правиле.

Пример 141 – Установка внутреннего IP-адреса для настройки DNAT

```
admin@edge# set service nat ipv4 rule 15 inside-address address 192.168.10.1
```

В примере ниже показано применение правила 15, которое будет подставлять адреса от 192.168.10.1 до 192.168.10.3 в качестве IP-адресов получателя для входящих пакетов, удовлетворяющих условиям правила.

Пример 142 – Установка диапазона внутренних адресов для настройки DNAT

```
admin@edge# set service nat ipv4 rule 15 inside-address address 192.168.10.1-
192.168.10.3
```

Внешний адрес

Параметр outside-address используется для настройки преобразования сетевого адреса отправителя (SNAT). Он позволяет определить адрес, который будет использоваться для замены IP-адреса отправителя исходящих пакетов. Также может использоваться преобразование номеров портов (port translation), номер сетевого порта указывается как часть определяемого внешнего адреса.

Необходимо учитывать следующее:

- Указание внешнего адреса является обязательным для правил преобразования отправителя (SNAT).
- Внешним адресом должен быть один из адресов, назначенных выходному интерфейсу.
- Внешний адрес *не может быть указан* для правил "маскировки" (тип **masquerade**). Так как при маскировке используется основной IP-адрес выходного интерфейса. Однако для правил "маскировки" (тип **masquerade**) может быть указан номер сетевого порта.

В примере ниже настраивается применение правила 10, которое осуществляет подстановку адреса 192.168.10.254 в качестве IP-адреса отправителя для сетевых пакетов, удовлетворяющих условиям правила.

Пример 143 – Установка внешнего адреса для настройки SNAT

```
admin@edge# set service nat ipv4 rule 10 outside-address address
192.168.10.254
```

В примере ниже показано применение правила 10 для подстановки адресов от 192.168.10.252 до 192.168.10.254 в качестве IP-адресов отправителя для исходящих пакетов, удовлетворяющих критерию правила.

Пример 144– Установка диапазона внешних адресов для настройки SNAT

```
admin@edge# set service nat ipv4 rule 15 outside-address address
192.168.10.252-192.168.10.254
```

18.2.5 Настройка интерфейсов

Для правил преобразования сетевых адресов (NAT) можно указать интерфейс, через который пакеты будут отправляться, или интерфейс, на котором сетевые пакеты будут приниматься. Необходимо учитывать следующее:

- Для правила преобразования адреса получателя (тип **destination**) (DNAT) указывается входной интерфейс. Интерфейс, через который входящий трафик попадает в устройство, осуществляющее преобразование сетевых адресов.
- Для правил преобразования сетевого адреса отправителя (тип **source**) (SNAT) указывается выходной интерфейс. Это интерфейс, через который исходящий трафик покидает устройство, осуществляющее преобразование сетевых адресов.
- Для правил "маскировки" (тип **masquerade**), указывается выходной интерфейс. Это интерфейс, через который исходящий трафик покидает устройство, осуществляющее преобразование сетевых адресов.

В примере ниже для правила 15 указывается, что для принятия входящего трафика будет прослушиваться интерфейс eth0.

Пример 145– Установка входного интерфейса для правила DNAT

```
admin@edge# set service nat ipv4 rule 15 inbound-interface eth0
```

В примере ниже для правила 10 устанавливается отправка исходящего трафика через интерфейс eth1.

Пример 146– Установка выходного интерфейса для правила SNAT

```
admin@edge# set service nat ipv4 rule 10 outbound-interface eth1
```

18.2.6 Итоговая конфигурация

Итоговая конфигурация будет выглядеть следующим образом:

```
admin@edge# show service nat
   ipv4 {
      rule 10 {
         destination {
            address 192.168.11.254
         }
         outbound-interface eth1
         outside-address {
            address 192.168.10.254
         }
         source {
            address 192.168.11.1
         }
         type source
      }
      rule 15 {
         inbound-interface eth0
         inside-address {
            address 192.168.10.1
         }
         protocol tcp
         source {
            address 192.168.11.0/24
            port 80
         }
         type destination
      }
   }
```

18.3 Примеры настройки NAT

В этом разделе приведены примеры настройки преобразования сетевых адресов (NAT).

ПРИМЕЧАНИЕ Правила, используемые в данных примерах, должны быть развернуты в системе независимо друг от друга. Совместное использование данных примеров не предполагается. По этой причине, все правила в примерах имеют одни и те же номера (правило 10).

В этом разделе рассматриваются следующие вопросы:

- Преобразование сетевого адреса отправителя (один к одному).
- Преобразование сетевого адреса отправителя (многие к одному).
- Преобразование сетевого адреса отправителя (многие ко многим).
- Преобразование сетевого адреса отправителя (один ко многим).

- Маскировка.
- Преобразование сетевого адреса получателя (один к одному).
- Преобразование сетевого адреса получателя (один ко многим).
- Двунаправленное преобразование сетевых адресов.
- Сопоставление диапазонов адресов.
- Макскировка и VPN.
- Параметр "exclude".

18.3.1 Преобразование сетевого адреса отправителя (один к одному)

На рисунке ниже приведен пример преобразования сетевого адреса отправителя (SNAT), в котором единственный "внутренний" адрес отправителя заменяется на единственный "внешний" адрес отправителя. В этом примере:

- Внутренний новостной сервер (NNTP), которому требуется устанавливать подключение ко внешнему новостному серверу.
- Внешний новостной сервер принимает подключения только от известных клиентов.
- Внутренний новостной сервер не принимает подключения извне локальной сети.

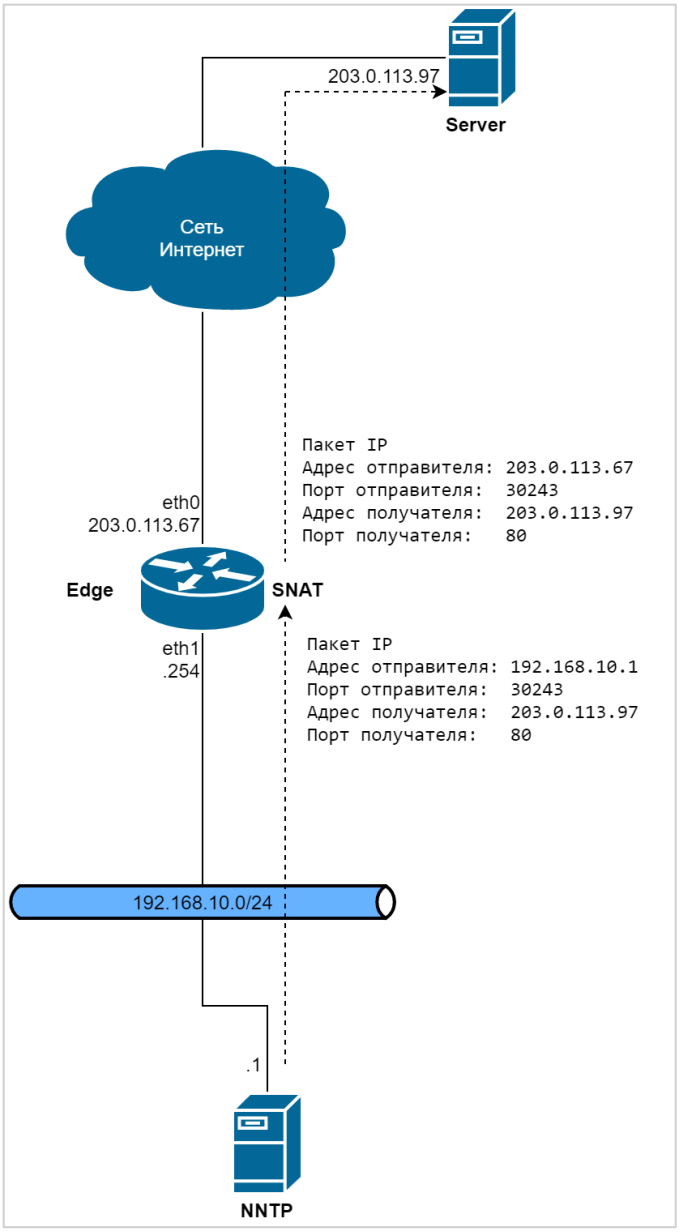


Рисунок 27 – Настройка SNAT (один к одному)

Для настройки преобразования сетевых адресов в соответствии с данным рисунком нужно выполнить следующие действия в режиме настройки.

Пример 147 – Настройка SNAT (один к одному)

Действие	**Команда**
Создание правила 10. Правило 10 является правилом преобразования сетевого адреса отправителя (SNAT).	`[edit]` `admin@edge# set service nat ipv4 rule 10 type source`
Применение правила к сетевым пакетам, отправленным с узла 192.168.10.1.	`[edit]` `admin@edge# set service nat ipv4 rule 10 source address 192.168.10.1`

Отправка трафика через интерфейс eth0. Адрес 203.0.113.67 используется в качестве адреса отправителя для исходящих сетевых пакетов. Следует учесть, что внешний адрес должен быть одним из адресов, назначенных выходному интерфейсу.	`[edit]`
	`admin@edge# set service nat ipv4 rule 10 outbound-interface eth0`
	`[edit]`
	`admin@edge# set service nat ipv4 rule 10 outside-address address 203.0.113.67`

Фиксация изменения.	`[edit]` `admin@edge# commit`

Вывод настройки.	`[edit]`
	`admin@edge# show service nat ipv4 rule 10`
	`  outbound-interface eth0`
	`  outside-address {`
	`  address 203.0.113.67`
	`  }`
	`  source {`
	`  address 192.168.10.1`
	`  }`
	`  type source`

18.3.2 Преобразование сетевого адреса отправителя (многие к одному)

На рисунке ниже приведен пример преобразования сетевого адреса отправителя, где несколько различных "внутренних" адресов динамически заменяются на один "внешний" адрес. В этом примере все узлы подсети 192.168.10.0/24 будут использовать один и тот же внешний адрес отправителя.

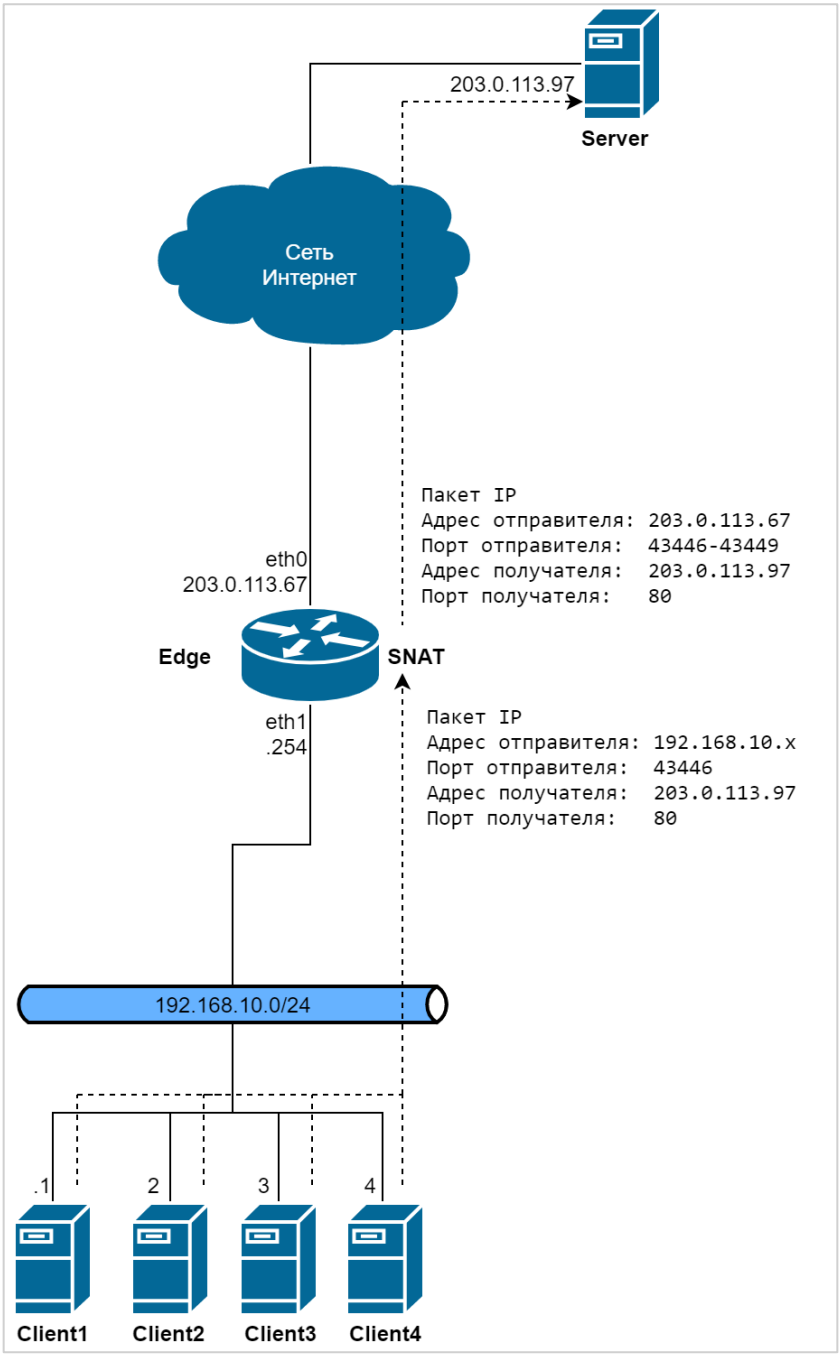


Рисунок 28 – Настройка SNAT (многие к одному)

Для настройки преобразования сетевых адресов в соответствии с данным рисунком нужно выполнить следующие действия в режиме настройки.

Пример 148 – Настройка SNAT (многие к одному)

Действие	**Команда**
Создание правила 10. Правило 10 является правилом преобразования сетевого адреса отправителя (SNAT).	`[edit]` `admin@edge# set service nat ipv4 rule 10 type source`
Применение данного правила к пакетам, которые были отправлены любым узлом сети 192.168.10.0/24.	`[edit]` `admin@edge# set service nat ipv4 rule 10 source address 192.168.10.0/24`

Отправка трафика через интерфейс eth0. Адрес 203.0.113.67 используется в качестве адреса отправителя для исходящих сетевых пакетов. Следует учесть, что внешний адрес должен быть	`[edit]`
	`admin@edge# set service nat ipv4 rule 10 outbound-interface eth0`
	`[edit]`

Действие	Команда
одним из адресов, определенных на выходном интерфейсе.	admin@edge# set service nat ipv4 rule 10 outside-address address 203.0.113.67
Фиксация изменения.	[edit] admin@edge# commit

Вывод настройки.	[edit]
	admin@edge# show service nat ipv4 rule 10
	outbound-interface eth0
	outside-address {
	address 203.0.113.67
	}
	source {
	address 192.168.10.0/24
	}
	type source

18.3.3 Преобразование сетевого адреса отправителя (многие ко многим)

В преобразованиях типа "многие ко многим" набор частных IP-адресов заменяется на набор общедоступных адресов. На рисунке ниже несколько пространств частных адресов преобразуется в несколько внешних адресов.

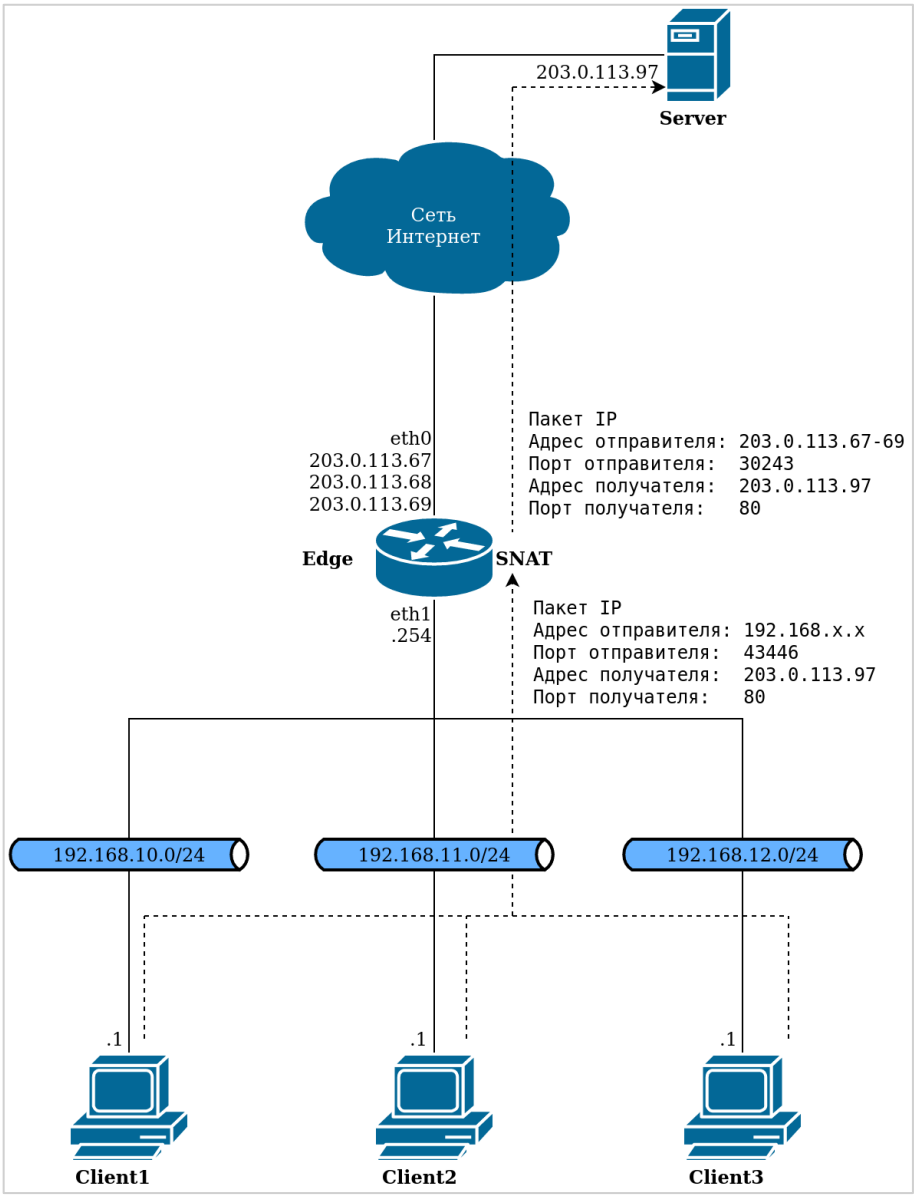


Рисунок 29 – Настройка SNAT (многие ко многим)

Для настройки преобразования сетевых адресов в соответствии с данным рисунком нужно выполнить следующие действия в режиме настройки.

Пример 149 – Настройка SNAT (многие ко многим)

Действие	**Команда**
Создание правила 10. Правило 10 является правилом преобразования сетевого адреса отправителя (SNAT).	`[edit]` `admin@edge# set service nat ipv4 rule 10 type source`
Применение данного правила к пакетам, которые были отправлены любым узлом сети 192.168.0.0/16.	`[edit]` `admin@edge# set service nat ipv4 rule 10 source address 192.168.0.0/16`

Отправка сетевого трафика через интерфейс eth0. Выбор адреса в диапазоне от 203.0.113.67 до 203.0.113.69 в качестве адреса отправителя исходящих пакетов. Следует отметить, что внешние адреса должны быть определены на выходном интерфейсе.	`[edit]`
	`admin@edge# set service nat ipv4 rule 10 outbound-interface eth0`
	`[edit]`
	`admin@edge# set service nat ipv4 rule 10 outside-address address 203.0.113.67-203.0.113.69`

Фиксация изменения.	`[edit]` `admin@edge# commit`

Вывод настройки.	`[edit]`
	`admin@edge# show service nat ipv4 rule 10`
	`  outbound-interface eth0`
	`  outside-address {`
	`  address 203.0.113.67-203.0.113.69`
	`  }`
	`  source {`
	`  address 192.168.0.0/16`
	`  }`
	`  type source`

18.3.4 Преобразование сетевого адреса отправителя (один ко многим)

Эта схема менее распространена. Одним из вариантов применения данной схемы может быть тестирование устройства балансировки нагрузки в сеть верхнего уровня (upstream load-balancing device). В данной схеме единственное устройство, расположенное за устройством, осуществляющим преобразование сетевых адресов, для внешней сети предстает как несколько устройств.

Для настройки преобразования сетевых адресов в соответствии с данным рисунком нужно выполнить следующие действия в режиме настройки.

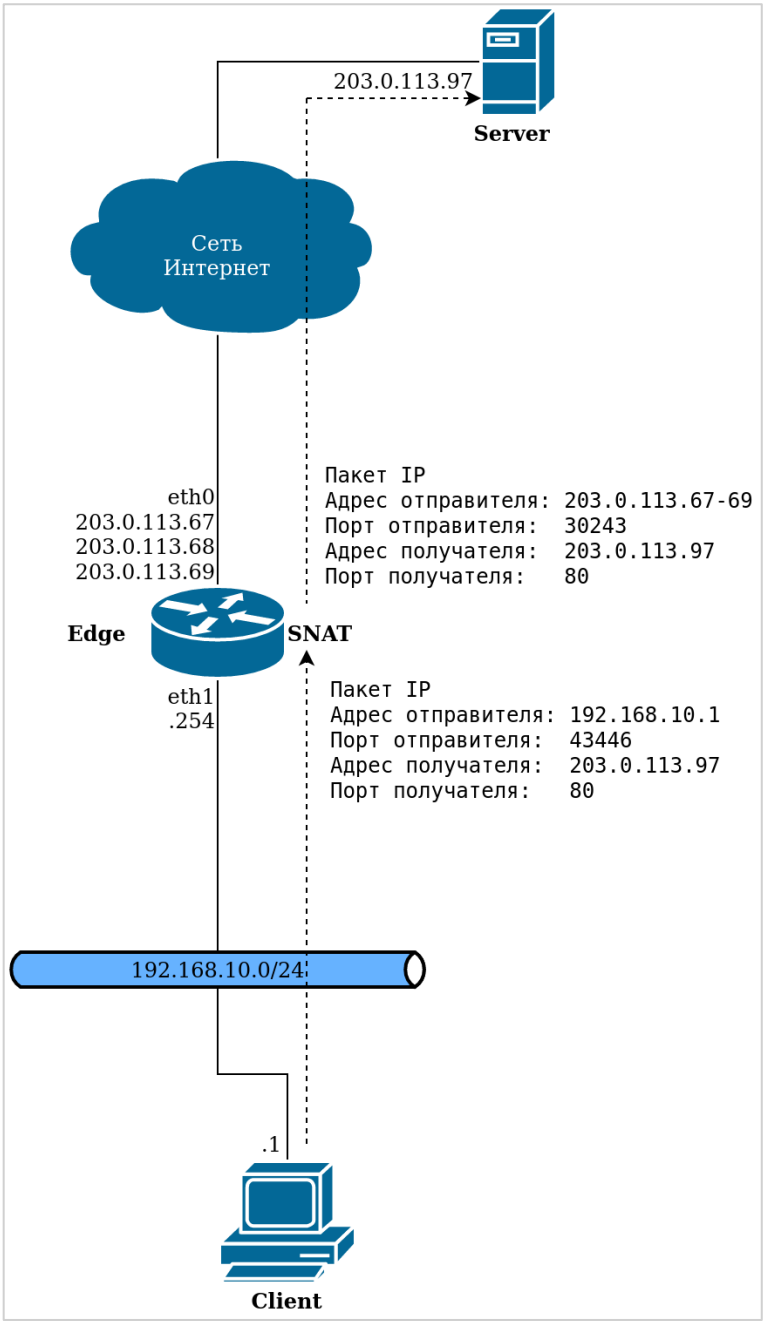


Рисунок 30– Настройка SNAT (один ко многим)

Пример 150 – Преобразование сетевого адреса отправителя (один ко многим)

Действие	**Команда**
Создание правила 10. Правило 10 является правилом преобразования сетевого адреса отправителя (SNAT).	`[edit]` `admin@edge# set service nat ipv4 rule 10 type source`
Применение правила к сетевым пакетам, отправленным с узла 192.168.10.1.	`[edit]` `admin@edge# set service nat ipv4 rule 10 source address 192.168.10.1`

Отправка сетевого трафика через интерфейс eth0. Выбор адреса в диапазоне от 203.0.113.67 до 203.0.113.69 в качестве адреса отправителя исходящих пакетов. Следует отметить, что внешние адреса должны быть определены на выходном интерфейсе.	`[edit]`
	`admin@edge# set service nat ipv4 rule 10 outbound-interface eth0`
	`[edit]`
	`admin@edge# set service nat ipv4 rule 10 outside-address address 203.0.113.67-203.0.113.69`

Фиксация изменения.	`[edit]`

Действие	Команда
	admin@edge# commit

Вывод настройки.	[edit]
	admin@edge# show service nat ipv4 rule 10
	outbound-interface eth0
	outside-address {
	address 203.0.113.67-203.0.113.69
	}
	source {
	address 192.168.10.1
	}
	type source

18.3.5 Маскировка

При использовании маскировки (частный случай SNAT) адрес отправителя исходящего пакета заменяется основным IP-адресом выходного интерфейса. Это необходимо, когда адрес выходного интерфейса предоставляется по DHCP и с окончанием периода аренды может измениться. Данный механизм предназначен для решения проблем организации связи между сетевыми устройствами и узлами, которым назначены частные (RFC 1918) IP-адреса, так как в противном случае пакеты IP не смогут быть переданы через Интернет.

Правила "маскировки" состоят из условий, на основе которых осуществляется проверка соответствия:

- Сеть отправителя (обычно частный IP-адрес локальной сети, в которой расположены устройства).
- Сеть получателя (обычно 0.0.0.0/0, которая используется для обозначения любого адреса).
- Выходной интерфейс (пограничный интерфейс, которому назначен общедоступный адрес).

При установлении соответствия сетевого пакета правилу "маскировки" адрес отправителя сетевого пакета изменяется до того, как будет осуществлена пересылка пакета получателю.

В этой схеме ряду узлов требуется инициировать сеансы связи со внешними устройствами, но при этом доступен только один общедоступный (public) IP-адрес. Это может потребоваться, например, в случае, если для организации связи используется последовательный интерфейс. На рисунке ниже приведен пример использования "маскировки".

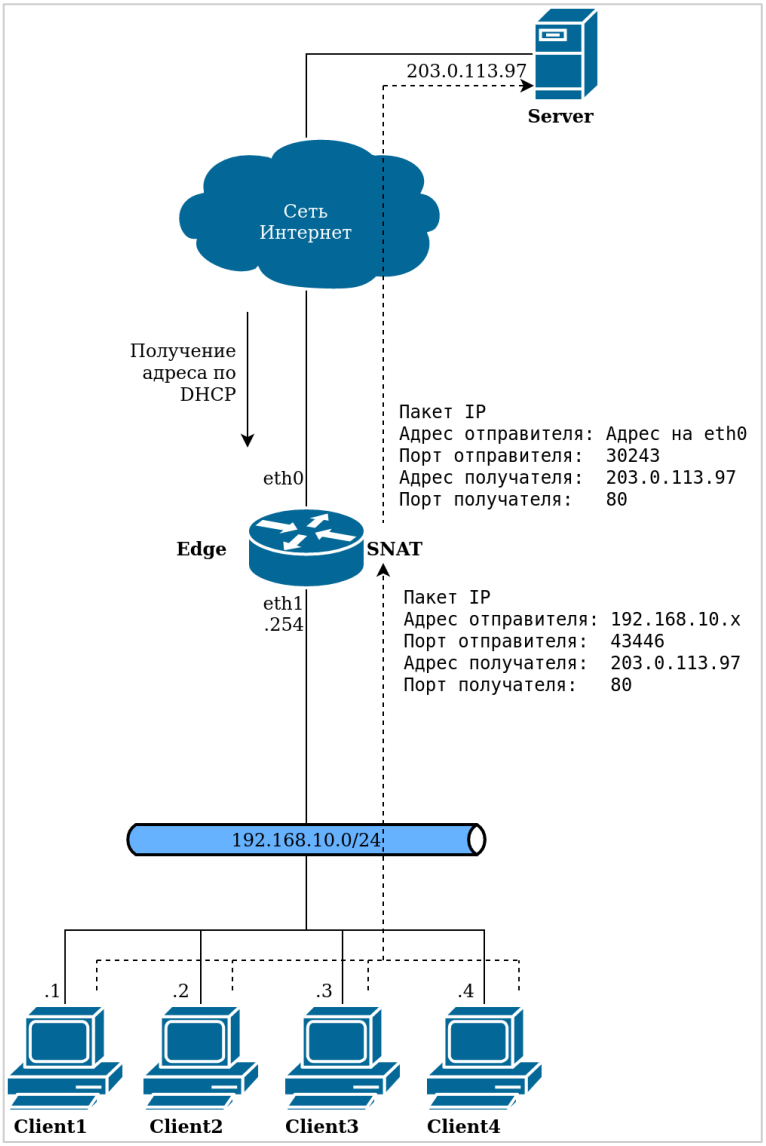


Рисунок 31 – Маскировка

Для настройки преобразования сетевых адресов в соответствии с данным рисунком нужно выполнить следующие действия в режиме настройки.

Пример 151– Маскировка

Действие	**Команда**
Создание правила 10. Правило 10 является правилом преобразования сетевого адреса отправителя (SNAT).	`[edit]` `admin@edge# set service nat ipv4 rule 10 type masquerade`
Применение данного правила к пакетам, которые были отправлены любым узлом сети 192.168.10.0/24.	`[edit]` `admin@edge# set service nat ipv4 rule 10 source address 192.168.10.0/24`
Отправка сетевого трафика через интерфейс eth0. Использование IP-адреса выходного интерфейса в качестве внешнего адреса.	`[edit]` `admin@edge# set service nat ipv4 rule 10 outbound-interface eth0`
Фиксация изменения.	`[edit]` `admin@edge# commit`

Вывод настройки.	`admin@edge# show service nat ipv4 rule 10`
	`  outbound-interface eth0`
	`  source {`
	`  address 192.168.10.0/24`
	`  }`

Действие	Команда
	type masquerade

18.3.6 Преобразование сетевого адреса получателя (один к одному)

Преобразование сетевого адреса получателя (DNAT) используется только в тех случаях, когда необходимо принимать входящий трафик.

Схема 1: Сетевые пакеты, предназначенные для внутреннего веб-сервера

Например, преобразование сетевого адреса получателя может быть использовано в том случае, если в корпоративной сети есть веб-сервер, который принимает подключения от устройств внешней сети, но при этом не инициирует исходящих сеансов.

Для настройки преобразования сетевых адресов в соответствии с данным рисунком нужно выполнить следующие действия в режиме настройки.

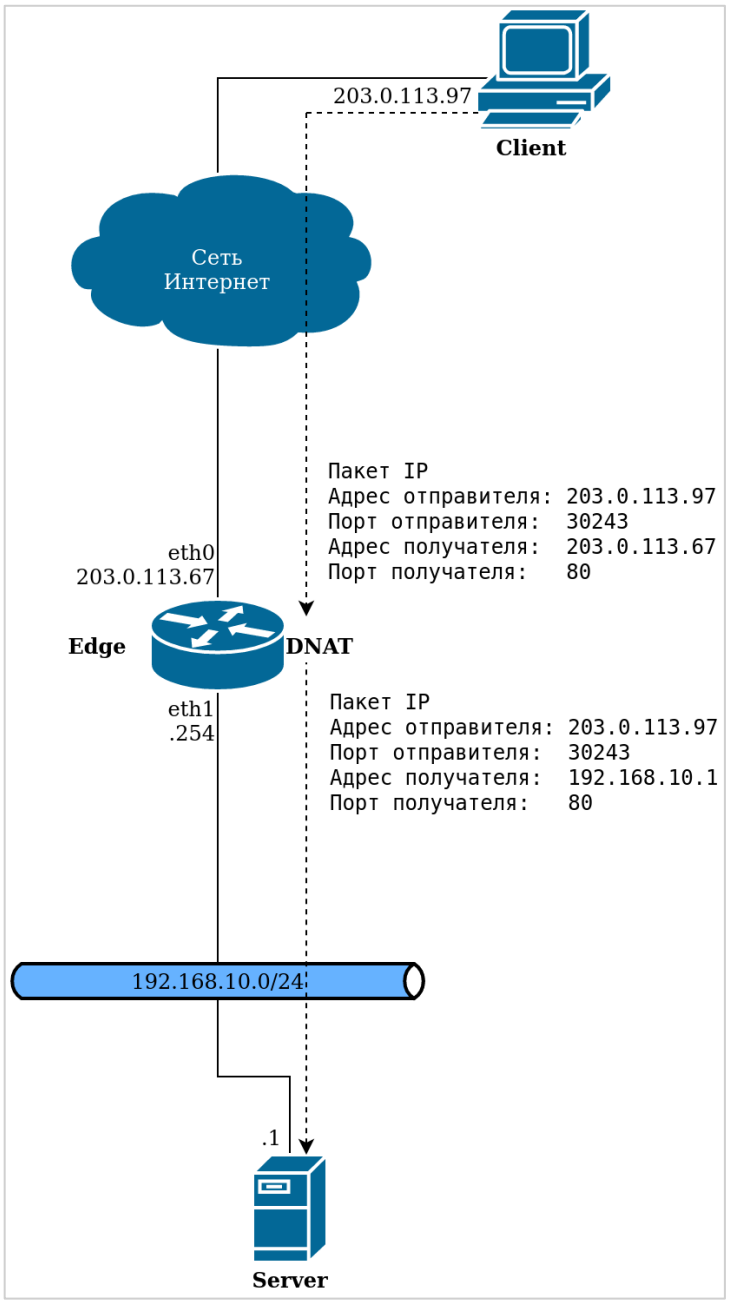


Рисунок 32 – Настройка DNAT (один к одному)

Пример 152 – Преобразование сетевого адреса получателя (один к одному)

Действие	**Команда**
Создание правила 10. Правило 10 является правилом преобразования сетевого адреса получателя (DNAT).	`[edit]` `admin@edge# set service nat ipv4 rule 10 type destination`

Применение данного правила ко всем входящим пакетам TCP на интерфейсе eth0 для адреса 203.0.113.67 и порта HTTP.	`[edit]`
	`admin@edge# set service nat ipv4 rule 10 inbound-interface eth0`
	`[edit]`
	`admin@edge# set service nat ipv4 rule 10 destination address 203.0.113.67`
	`[edit]`
	`admin@edge# set service nat ipv4 rule 10 protocol tcp`
	`[edit]`
	`admin@edge# set service nat ipv4 rule 10 destination port http`

Пересылка трафика на адрес 192.168.10.1.	`[edit]` `admin@edge# set service nat ipv4 rule 10 inside-address address 192.168.10.1`
Фиксация изменения.	`[edit]` `admin@edge# commit`

Вывод настройки.	`[edit]`
	`admin@edge# show service nat ipv4 rule 10`
	`  destination {`
	`  address 203.0.113.67`
	`  port http`
	`  }`
	`  inbound-interface eth0`
	`  inside-address {`
	`  address 192.168.10.1`
	`  }`
	`  protocols tcp`
	`  type destination`

Схема 2: Сетевые пакеты, предназначенные внутреннему серверу SSH

В этой схеме весь сетевой трафик, приходящий на порт SSH, направляется узлу, на котором функционирует сервер SSH.

Для настройки преобразования сетевых адресов в соответствии с данным рисунком нужно выполнить следующие действия в режиме настройки.

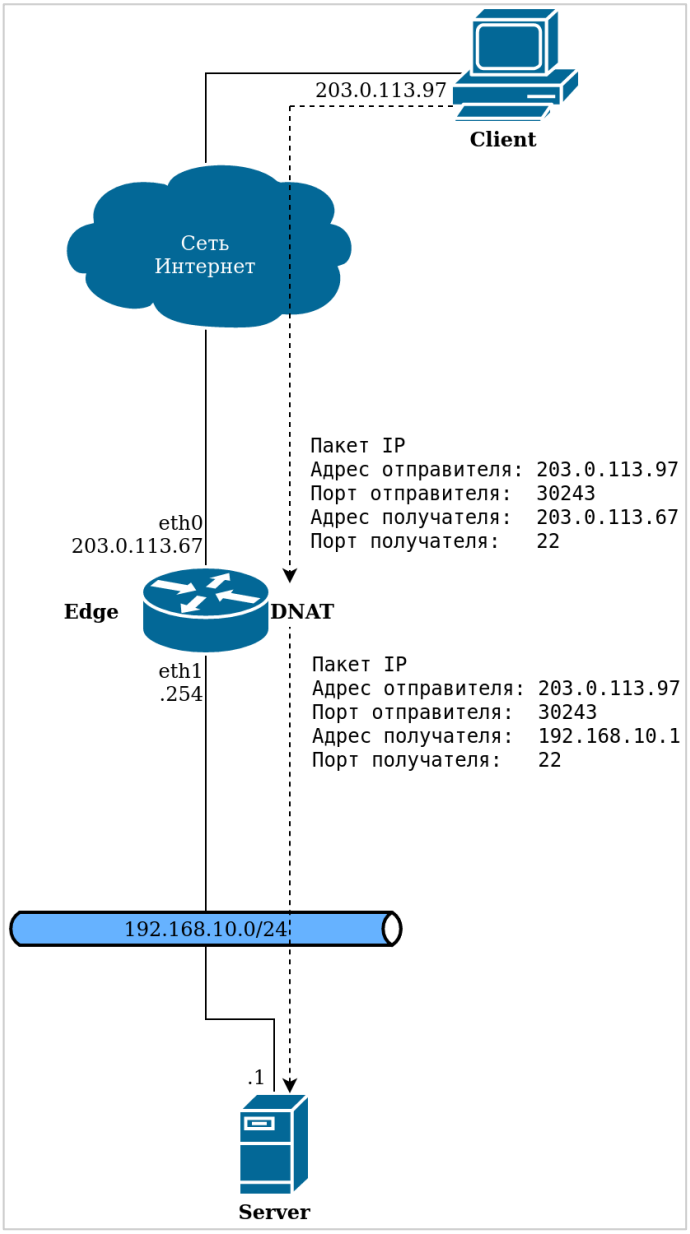


Рисунок 33 – Настройка DNAT (один к одному) - фильтрация по имени порта

Пример 153– Настройка DNAT (один к одному) - фильтрация по имени порта

Действие	**Команда**
Создание правила 10. Правило 10 является правилом преобразования сетевого адреса получателя (DNAT).	`[edit]a` `dmin@edge# set service nat ipv4 rule 10 type destination`

Применение данного правила ко всем входящим пакетам на интерфейсе eth0 для адреса 203.0.113.67 и порта SSH.	`[edit]`
	`admin@edge# set service nat ipv4 rule 10 inbound-interface eth0`
	`[edit]`
	`admin@edge# set service nat ipv4 rule 10 protocol tcp`
	`[edit]`
	`admin@edge# set service nat ipv4 rule 10 destination port ssh`
	`[edit]`
	`admin@edge# set service nat ipv4 rule 10 destination address 203.0.113.67`

Пересылка трафика на адрес 192.168.10.1.	`[edit]` `admin@edge# set service nat ipv4 rule 10`

Действие	Команда
	`inside-address address 192.168.10.1`
Фиксация изменения.	`[edit]` `admin@edge# commit`

Вывод настройки.	`[edit]`
	`admin@edge# show service nat ipv4 rule 10`
	`  destination {`
	`  address 203.0.113.67`
	`  port ssh`
	`  }`
	`  inbound-interface eth0`
	`  inside-address {`
	`  address 192.168.10.1`
	`  }`
	`  protocols tcp`
	`  type destination`

18.3.7 Преобразование сетевого адреса получателя (один ко многим)

Другой вариант применения преобразования сетевого адреса получателя, когда доступ к корпоративным ресурсам извне осуществляется через один IP-адрес (то есть единственный IP-адрес динамически отображается на несколько IP-адресов), приведен на рисунке ниже.

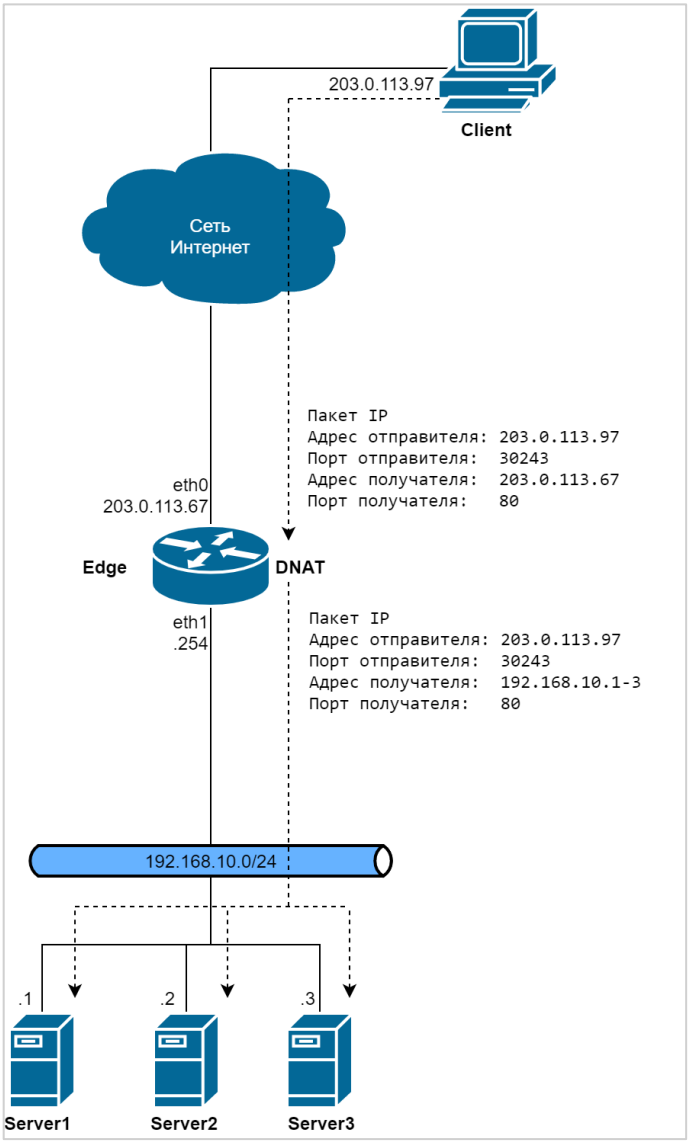


Рисунок 34 – Настройка DNAT (один ко многим)

Для настройки преобразования сетевых адресов в соответствии с данным рисунком нужно выполнить следующие действия в режиме настройки.

Пример 154– Настройка DNAT (один ко многим)

Действие	**Команда**
Создание правила 10. Правило 10 является правилом преобразования сетевого адреса получателя (DNAT).	`[edit]` `admin@edge# set service nat ipv4 rule 10 type destination`

Применение данного правила на интерфейсе eth0 для адреса 203.0.113.67.	`[edit]`
	`admin@edge# set service nat ipv4 rule 10 inbound-interface eth0`
	`[edit]`
	`admin@edge# set service nat ipv4 rule 10 destination address 203.0.113.67`

Пересылка трафика на адреса из диапазона от 192.168.10.1 до 192.168.10.3.	`[edit]` `admin@edge# set service nat ipv4 rule 10 inside-address address 192.168.10.1-192.168.10.3`
Фиксация изменения.	`[edit]` `admin@edge# commit`

Вывод настройки.	`admin@edge# show service nat ipv4 rule 10`
	`destination {`
	`address 203.0.113.67`
	`}`
	`inbound-interface eth0`
	`inside-address {`
	`address 192.168.10.1-192.168.10.3`
	`}`
	`type destination`

18.3.8 Двунаправленное преобразование сетевых адресов

Двунаправленное преобразование сетевых адресов представляет собой сочетание преобразования сетевого адреса отправителя и адреса получателя. Обычно преобразование сетевых адресов отправителя применяется к исходящему трафику всей частной сети, а преобразование сетевых адресов получателя только для конкретных внутренних служб (например, для почтовых и веб-серверов).

Для настройки преобразования сетевых адресов в соответствии с данным рисунком нужно выполнить следующие действия в режиме настройки.

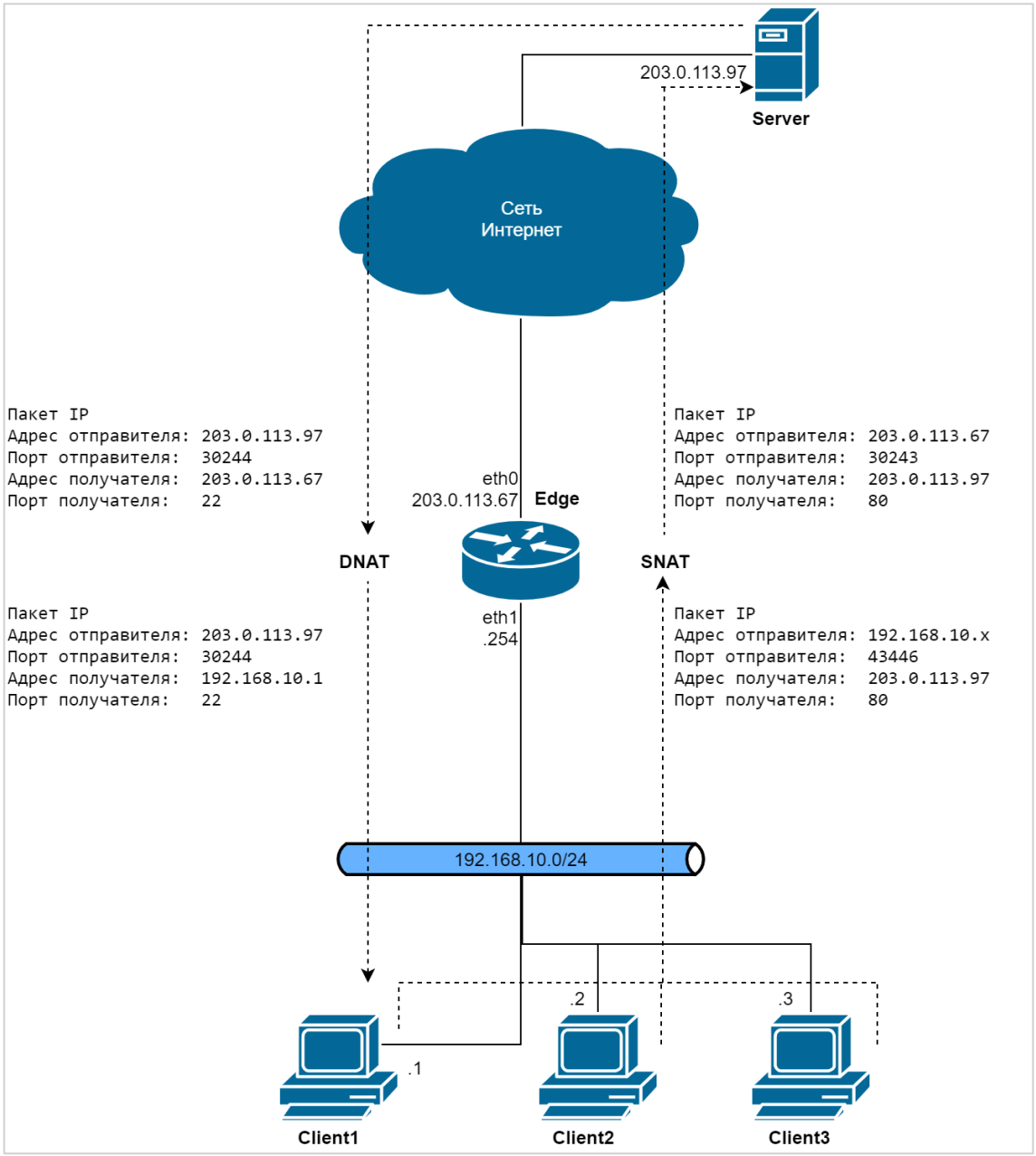


Рисунок 35 – Двунаправленное преобразование сетевых адресов

Пример 155– Двунаправленное преобразование сетевых адресов

Действие	**Команда**
Создание правила 10. Правило 10 является правилом преобразования сетевого адреса отправителя (SNAT).	`[edit]` `admin@edge# set service nat ipv4 rule 10 type source`
Применение данного правила к пакетам, отправленным любым узлом сети 192.168.10.0/24.	`[edit]` `admin@edge# set service nat ipv4 rule 10 source address 192.168.10.0/24`

Отправка трафика через интерфейс eth0. Использование адреса 203.0.113.67 в качестве адреса отправителя для исходящих пакетов.	`[edit]`
	`admin@edge# set service nat ipv4 rule 10 outbound-interface eth0`
	`[edit]`
	`admin@edge# set service nat ipv4 rule 10 outside-address address 203.0.113.67`

Создание правила 20. Правило 20 является правилом преобразования сетевого адреса получателя (DNAT).	`[edit]` `admin@edge# set service nat ipv4 rule`

Действие	Команда
	20 type destination
Применение данного правила на интерфейсе eth0 для адреса 203.0.113.67.	[edit] admin@edge# set service nat ipv4 rule 20 inbound-interface eth0 [edit] admin@edge# set service nat ipv4 rule 20 destination address 203.0.113.67
Пересылка трафика на адрес 192.168.10.1.	admin@edge# set service nat ipv4 rule 20 inside-address address 192.168.10.1
Фиксация изменения.	[edit] admin@edge# commit

Вывод настройки.	[edit]
	admin@edge# show service nat ipv4 rule 10
	outbound-interface eth0
	outside-address {
	address 203.0.113.67
	}
	source {
	address 192.168.10.0/24
	}
	type source
	[edit]
	admin@edge# show service nat ipv4 rule 20
	destination {
	address 203.0.113.67
	}
	inbound-interface eth0
	inside-address {
	address 192.168.10.1
	}
	type destination

18.3.9 Сопоставление диапазонов адресов

Возможно сопоставление адресов одной сети с адресами другой сети. Например, можно сопоставить адреса сети 192.168.10.0/24 с адресами сети 203.0.113.0/24, то есть адрес 192.168.10.1 будет сопоставлен с адресом 203.0.113.1, адрес 192.168.10.2 будет сопоставлен с адресом 203.0.113.2 и т.д. Сети должны быть одного размера, то есть они должны иметь одинаковые маски подсети.

В предположении, что подключения могут быть инициированы из обеих сетей, для настройки необходимо выполнить следующие действия в режиме настройки.

Пример 156– Сопоставление диапазонов адресов

Действие	Команда
Создание правила 10. Правило 10 является правилом преобразования сетевого адреса отправителя (SNAT).	[edit] admin@edge# set service nat ipv4 rule 10 type source
Применение данного правила к пакетам, отправленным любым узлом сети 192.168.10.0/24.	[edit] admin@edge# set service nat ipv4 rule 10 source address 192.168.10.0/24
Отправка трафика через интерфейс eth0. Использование адреса 203.0.113.*x* в качестве адреса отправителя для исходящих пакетов.	[edit] admin@edge# set service nat ipv4 rule 10 outbound-interface eth0 [edit] admin@edge# set service nat ipv4 rule 10 outside-address address 203.0.113.0/24
Создание правила 20. Правило 20 является правилом	[edit]

Действие	Команда
преобразования сетевого адреса отправителя (SNAT).	admin@edge# set service nat ipv4 rule 20 type source
Применение данного правила к пакетам, отправленным любым узлом сети 203.0.113.0/24.	[edit] admin@edge# set service nat ipv4 rule 20 source address 203.0.113.0/24
Отправка трафика через интерфейс eth1. Использование адреса 192.168.10.*x* в качестве адреса отправителя для исходящих пакетов.	[edit] admin@edge# set service nat ipv4 rule 20 outbound-interface eth1 [edit] admin@edge# set service nat ipv4 rule 20 outside-address address 192.168.10.0/24
Фиксация изменения.	[edit] admin@edge# commit

Вывод настройки.	[edit]
	admin@edge# show service nat ipv4 rule 10
	outbound-interface eth0
	outside-address {
	address 203.0.113.0/24
	}
	source {
	address 192.168.10.0/24
	}
	type source
	[edit]
	admin@edge# show service nat ipv4 rule 20
	outbound-interface eth1
	outside-address {
	address 192.168.10.0/24
	}
	source {
	address 203.0.113.0/24
	}
	type source

Если подключения инициируются только узлами сети 192.168.10.0/24, тогда требуется только правило 10. Если подключения инициируются только узлами сети 203.0.113.0/24, то требуется только правило 20.

Сопоставление сетей осуществляется аналогично преобразованию сетевых адресов получателя (DNAT).

18.3.10 Маскировка и VPN

При установлении соответствия сетевого пакета правилу "маскировки" адрес отправителя сетевого пакета изменяется до того, как будет осуществлена пересылка пакета получателю. Это означает, что правила "маскировки" применяются до того, как процесс VPN обрабатывает пакеты в соответствии с настройкой. Если сеть отправителя, для которой настроена "маскировка", также подключена к другой сети с помощью VPN через один и тот же внешний интерфейс, сетевые пакеты не будут обработаны процессом VPN (так как адрес отправителя будет изменен) и соответственно не будут отправлены через туннель VPN.

Чтобы исключить такое поведение, для пакетов, которые должны быть отправлены через туннель VPN, не должно выполняться преобразование адресов, для этого используется "исключающее правило" (правило, в котором используется операция отрицания [“!”]).

Для настройки правил маскировки в обход туннеля VPN нужно выполнить следующие действия в режиме настройки.

Пример 157– Настройка правил маскировки в обход туннеля VPN

Действие	Команда
Создание правила 10. Правило 10 является правилом преобразования сетевого адреса отправителя (SNAT).	[edit] admin@edge# set service nat ipv4 rule 10 type masquerade

Действие	Команда
Применение данного правила к сетевым пакетам, которые были отправлены любым узлом сети 192.168.0.0/16.	[edit] admin@edge# set service nat ipv4 rule 10 source address 192.168.0.0/16
Применение данного правила ко всем сетевым пакетам, кроме пакетов, предназначенных сети для сети 203.0.113.98/32.	[edit] admin@edge# set service nat ipv4 rule 10 destination address !203.0.113.98/32
Отправка сетевого трафика через интерфейс eth0. Использование IP-адреса выходного интерфейса в качестве внешнего адреса.	[edit] admin@edge# set service nat ipv4 rule 10 outbound-interface eth0
Фиксация изменения.	[edit] admin@edge# commit

Вывод настройки.	[edit]
	admin@edge# show service nat ipv4 rule 10
	destination {
	address !203.0.113.98/32
	}
	outbound-interface eth0
	source {
	address 192.168.0.0/16
	}
	type masquerade

Следует отметить, что необходимо использовать "исключающие" правила с особой осторожностью. Правила NAT выполняются по порядку, и при использовании набора правил, содержащего более одного "исключающего" правила, могут быть получены результаты, отличные от ожидаемых.

Рассмотрим правило преобразования адресов из примера ниже.

Пример 158– Единственное "исключающее правило": корректное поведение

Вывод настройки одного исключающего правила	[edit]
	admin@edge# show service nat ipv4
	rule 10 {
	destination {
	address !203.0.113.98/32
	}
	outbound-interface eth0
	source {
	address 192.168.10.0/24
	}
	type masquerade
	}

Это правило создает исключение для сети 203.0.113.98/32, как и требовалось. С другой стороны, рассмотрим набор из двух правил преобразований адресов в примере ниже.

Пример 159– Несколько "исключающих правил": поведение, отличное от ожидаемого

Вывод настройки двух исключающих правил	[edit]
	admin@edge# show service nat ipv4
	rule 10 {
	destination {
	address !203.0.113.98/32
	}
	outbound-interface eth0
	source {
	address 192.168.10.0/24
	}
	type masquerade
	}
	rule 20 {
	destination {
	address !203.0.113.99/32

```
      }
      outbound-interface eth0
      source {
         address 192.168.10.0/24
      }
      type masquerade
   }
```

В результате выполнения данного набора правил исключение для сетей 203.0.113.98/32 и 203.0.113.99/32 создано НЕ будет. Как указано выше, эти правила выполняются последовательно: при получении пакета он проверяется на соответствие первому правилу, если соответствие не установлено, он проверяется на соответствие второму правилу, и так до тех пор, пока не будет найдено соответствие.

В этом примере для пакета, имеющего сеть получателя 203.0.113.98/32, не будет установлено соответствие для правила 10 (которому будут соответствовать пакеты, сеть получателя которых отлична от 203.0.113.98). После чего пакет будут проверен на соответствие правилу 20. Для пакета, имеющего сеть получателя 203.0.113.98/32, будет установлено соответствие правилу 20 (так как адрес получателя отличен от сети 203.0.113.99/32), в результате для пакета будет выполнено преобразование сетевого адреса, что не является желаемым результатом.

Аналогично, пакет с сетью получателя 203.0.113.99/32 будет соответствовать правилу 10, в результате чего будет осуществлено преобразование адресов.

18.3.11 Параметр “exclude”

Также создать исключение для пакетов, для которых не следует осуществлять преобразование сетевых адресов, можно с помощью параметра **exclude**, который создает исключение для пакетов, для которых было установлено соответствие правилу NAT. В примере ниже используется параметр **exclude** для решения задачи.

Пример 160– Единственное исключающее правило: корректное поведение - использование параметра "exclude"

Вывод настройки одного правила с exclude

```
[edit]
admin@edge# show service nat ipv4
   rule 10 {
      destination {
         address 203.0.113.98/32
      }
      exclude outbound-interface eth0
      source {
         address 192.168.10.0/24
      }
      type masquerade
   }
   rule 20 {
      outbound-interface eth0
      source {
         address 192.168.10.0/24
      }
      type masquerade
   }
```

Дополнительное правило (правило 20) требуется для обработки пакетов, для которых не требуется создавать исключения.

В примере выше используется параметр **exclude**, чтобы получить результат, который не был получен в примере ниже. В этом примере правило 30 обрабатывает неисключенные пакеты.

Пример 161 – Использование нескольких исключающих правил: корректное поведение - использование параметра "exclude"

Вывод настройки двух правил с exclude

```
[edit]
admin@edge# show service nat ipv4
   rule 10 {
      destination {
         address 203.0.113.98/32
      }
```

	exclude outbound-interface eth0
	source {
	address 192.168.10.0/24
	}
	type masquerade
	}
	rule 20 {
	destination {
	address 203.0.113.99/32
	}
	exclude outbound-interface eth0
	source {
	address 192.168.10.0/24
	}
	type masquerade
	}
	rule 30 {
	outbound-interface eth0
	source {
	address 192.168.10.0/24
	}
	type masquerade
	}

18.4 Команды NAT

В этом разделе приведены команды преобразования сетевых адресов (NAT).

Команды настройки	
Команды настройки ipv4 NAT	
service nat ipv4	Включение преобразования сетевых адресов (NAT).
service nat ipv4 rule <номер_правила>	Определение правила преобразования сетевых адресов (NAT).
service nat ipv4 rule <номер_правила> description <описание>	Указание текстового описания для правила преобразования сетевых адресов (NAT).
service nat ipv4 rule <номер_правила> destination address <адрес>	Указание адреса получателя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).
service nat ipv4 rule <номер_правила> destination address-group <имя_группы_адресов>	Указание группы адресов для проверки соответствия адреса получателя сетевого пакета правилу преобразования сетевых адресов (NAT)
service nat ipv4 rule <номер_правила> destination address-type <тип_адреса>	Указание типа адреса получателя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).
service nat ipv4 rule <номер_правила> destination country <код_страны>	Указание двухзначного кода страны получателя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).
service nat ipv4 rule <номер_правила> destination domain-group <имя_группы_доменов>	Указание группы доменов для проверки соответствия адреса получателя сетевого пакета правилу преобразования сетевых адресов (NAT).
service nat ipv4 rule <номер_правила> destination network-group <имя_группы_сетей>	Указание группы сетей для проверки соответствия адреса получателя сетевого пакета правилу преобразования сетевых адресов (NAT).
service nat ipv4 rule <номер_правила> destination port-group <имя_группы_портов>	Указание группы сетевых портов для проверки соответствия адреса получателя сетевого пакета правилу преобразования сетевых адресов (NAT).
service nat ipv4 rule <номер_правила> destination port <порт>	Указание номера порта получателя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).

service nat ipv4 rule <номер_правила> disable	Отключение правила преобразования сетевых адресов (NAT).
service nat ipv4 rule <номер_правила> exclude	Создание правила, определяющего исключения для указанных пакетов, при преобразовании сетевых адресов (NAT).
service nat ipv4 rule <номер_правила> inbound-interface <интерфейс>	Указание входного интерфейса, на котором будет выполняться правило преобразования сетевого адреса получателя (DNAT).
service nat ipv4 rule <номер_правила> inside-address address <адрес>	Определение внутреннего адреса для правила, осуществляющего преобразование сетевого адреса получателя (DNAT).
service nat ipv4 rule <номер_правила> inside-address port <порт>	Определение внутреннего порта для правила, осуществляющего преобразование сетевого адреса получателя (DNAT).
service nat ipv4 rule <номер_правила> log <состояние>	Регистрация для правил преобразования сетевого адреса (NAT), для которых было установлено соответствие.
service nat ipv4 rule <номер_правила> outbound-interface <интерфейс>	Указание интерфейса, на который будет передаваться исходящий трафик для правил преобразования адресов отправителя (SNAT) и правил "маскировки" (masquerade).
service nat ipv4 rule <номер_правила> outside-address address <адрес>	Определение внешнего адреса для правила преобразования сетевого адреса отправителя (SNAT).
service nat ipv4 rule <номер_правила> outside-address <порт>	Определение внешнего порта для правила преобразования сетевого адреса отправителя (SNAT).
service nat ipv4 rule <номер_правила> protocol <протокол>	Указание протоколов, для которых осуществляется преобразование сетевых адресов (NAT).
service nat ipv4 rule <номер_правила> source adress <адрес>	Указание адреса отправителя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).
service nat ipv4 rule <номер_правила> source address-group <имя_группы_адресов>	Указание группы адресов для проверки соответствия адреса отправителя сетевого пакета правилу преобразования сетевых адресов (NAT).
service nat ipv4 rule <номер_правила> source address-type <тип_адреса>	Указание типа адреса отправителя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).
service nat ipv4 rule <номер_правила> source country <код_страны>	Указание двухзначного кода страны отправителя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).
service nat ipv4 rule <номер_правила> source domain-group <имя_группы_доменов>	Указание группы доменов для проверки соответствия адреса отправителя сетевого пакета правилу преобразования сетевых адресов (NAT).
service nat ipv4 rule <номер_правила> source network-group <имя_группы_сетей>	Указание группы сетей для проверки соответствия адреса отправителя сетевого пакета правилу преобразования сетевых адресов (NAT).
service nat ipv4 rule <номер_правила> source port-group <имя_группы_портов>	Указание группы сетевых портов для проверки соответствия адреса отправителя сетевого пакета правилу преобразования сетевых адресов (NAT).
service nat ipv4 rule <номер_правила> source port <порт>	Указание номера порта отправителя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).
service nat ipv4 rule <номер_правила> type <вид>	Установка вида преобразования для правила преобразования сетевого адреса (NAT).
Команды настройки Ethernet NAT	
service nat ethernet	Включение преобразования сетевых адресов (NAT) для протокола ethernet.
service nat ethernet rule <номер_правила>	Определение правила преобразования сетевых адресов (NAT) для протокола ethernet .

service nat ethernet rule <номер_правила> action <действие> to <mac-адрес>	Описание действия для правил преобразования сетевого адреса (NAT) для протокола ethernet, для которых было установлено соответствие.
service nat ethernet rule <номер_правила> description <описание>	Описание правила (NAT) для протокола ethernet.
service nat ethernet rule <номер_правила> destination ip <адрес>	Указание IP-адреса получателя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT) для протокола ethernet .
service nat ethernet rule <номер_правила> destination mac <mac-адрес>	Указание MAC-адреса получателя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT) для протокола ethernet .
service nat ethernet rule <номер_правила> disable	Отключение правила преобразования сетевых адресов (NAT) для протокола ethernet.
service nat ethernet rule <номер_правила> interface in <интерфейс>	Указание входного интерфейса, на котором будет выполняться правило преобразования сетевого адреса получателя (DNAT) и интерфейса.
service nat ethernet rule <номер_правила> interface out <интерфейс>	Указание исходящего интерфейса, на который будет передаваться исходящий трафик для правил преобразования адресов отправителя (SNAT).
service nat ethernet rule <номер_правила> log <состояние>	Регистрация для правил преобразования сетевого адреса (NAT) для протокола ethernet, для которых было установлено соответствие.
service nat ethernet rule <номер_правила> protocol <протокол>	Указание протоколов, для которых осуществляется преобразование сетевых адресов (NAT).
service nat ethernet rule <номер_правила> source ip <адрес>	Указание IP-адреса отправителя, по которым будет осуществляться проверка соответствия в правиле преобразования сетевого адреса (NAT) для протокола ethernet.
service nat ethernet rule <номер_правила> source mac <mac-адрес>	Указание MAC-адреса отправителя, по которым будет осуществляться проверка соответствия в правиле преобразования сетевого адреса (NAT) для протокола ethernet.
Эксплуатационные команды	
clear nat ipv4 counters	Очистка счетчиков для активных IPv4-правил преобразования сетевых адресов (NAT).
clear nat ethernet counters	Очистка счетчиков для активных Ethernet-правил преобразования сетевых адресов (NAT).
show nat ipv4 rules	Отображение настроенных правил преобразования сетевых адресов (NAT).
show nat ipv4 statistics	Вывод статистики для службы преобразования сетевых адресов (NAT).
show nat ipv4 translations	Вывод сведений о трансляциях сетевых адресов.
show nat ipv4 translations destination	Вывод сведений о трансляциях сетевых адресов получателя (DNAT).
show nat ipv4 translations source	Вывод сведений о трансляциях сетевых адресов отправителя (SNAT).
show nat ethernet rules	Отображение настроенных правил преобразования сетевых адресов (NAT) для протокола ethernet.
show nat ethernet statistics	Вывод статистики для службы преобразования сетевых адресов (NAT) для протокола ethernet.

18.4.1 service nat ipv4

Включение преобразования сетевых адресов (NAT).

Синтаксис

```
set service nat ipv4
delete service nat ipv4
show service nat ipv4
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   nat{
      ipv4 {
      }
   }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет включить преобразование сетевых адресов (NAT) в системе.

Форма **set** данной команды используется для создания и изменения настройки NAT.

Форма **delete** данной команды используется для удаления настройки NAT и отключения преобразования сетевых адресов в системе.

Форма **show** данной команды используется для отображения настройки NAT.

18.4.2 service nat ipv4 rule <номер_правила>

Определение правила преобразования сетевых адресов (NAT).

Синтаксис

```
set service nat ipv4 rule <номер_правила>
delete service nat ipv4 rule <номер_правила>
show service nat ipv4 rule <номер_правила>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   nat {
      ipv4 {
         rule номер_правила {
         }
      }
   }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания настройки правила преобразования сетевых адресов (NAT). Правила NAT исполняются в порядке следования их номеров. Следует отметить, что идентификатор правила NAT (номер правила) не может быть изменен после создания правила. Для обеспечения возможности вставки в будущем дополнительных правил, следует при назначении номеров правил оставлять интервалы; например, установить номера для начального набора правил: 10, 20, 30, 40, и т.д.

Форма **set** данной команды используется для создания и изменения правила NAT.

Форма **delete** данной команды используется для удаления правила NAT.

Форма **show** данной команды используется для отображения настройки правила NAT.

18.4.3 service nat ipv4 rule <номер_правила> description <описание>

Текстовое описание правила преобразования сетевых адресов .

Синтаксис

```
set service nat ipv4 rule <номер_правила> description <описание>
delete service nat ipv4 rule <номер_правила> description
show service nat ipv4 rule <номер_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   nat {
      ipv4 {
         rule номер_правила {
            description описание
         }
      }
   }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

описание

Мнемоническое имя или описание правила преобразования сетевых адресов .

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для установки текстового описания правила преобразования сетевых адресов.

Форма **set** данной команды используется для установки описания.

Форма **delete** данной команды используется для удаления описания.

Форма **show** данной команды используется для отображения настройки описания.

18.4.4 service nat ipv4 rule <номер_правила> destination address <адрес>

Указание адреса получателя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).

Синтаксис

```
set service nat ipv4 rule <номер_правила> destination address  <адрес>
delete service nat ipv4 rule <номер_правила> destination address
show service nat ipv4 rule <номер_правила> destination address
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   nat {
      ipv4 {
         rule номер_правила {
            destination {
               address адрес
            }
         }
      }
   }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

адрес

IPv4-адрес получателя для проверки соответствия. Допустимые форматы представлены в таблице ниже.

Таблица 132 – Форматы указания адреса получателя.

Значение	Описание
<x.x.x.x>	IPv4-адрес.
<x.x.x.x/x>	Подсеть адресов IPv4, где 0.0.0.0/0 соответствует любой сети.
<x.x.x.x>-<x.x.x.x>	Диапазон IPv4-адресов.
!<x.x.x.x>	Любой IPv4-адрес, КРОМЕ указанного.
!<x.x.x.x/x>	Любая подсеть адресов IPv4, КРОМЕ указанной подсети.
!<x.x.x.x>-<x.x.x.x>	Любые IPv4-адреса, КРОМЕ лежащих в указанном диапазоне.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда позволяет указать получателя, на основе которого будет осуществляться Установка соответствия в правиле NAT. Следует с осторожностью включать в набор правил более одного правила, определяющего исключения (правило, в котором указывается восклицательный знак "!"). Правила NAT выполняются по порядку, при этом последовательность правил, определяющих исключения, может привести к результатам, отличным от ожидаемых.

ПРИМЕЧАНИЕ Для указания адреса получателя адреса задаются либо указанием отдельного адреса, диапазона адресов или сетей данной командой, либо указанием группы адресов командой service nat ipv4 rule <номер_правила> destination address-group <имя_группы_адресов>. Параллельное использование обоих механизмов не допускается.

Форма **set** данной команды позволяет указать адрес получателя, используемый при преобразовании сетевых адресов.

Форма **delete** данной команды используется для удаления настройки адреса получателя NAT.

Форма **show** данной команды используется для отображения настройки адреса получателя NAT.

18.4.5 service nat ipv4 rule <номер_правила> destination address-group <имя_группы_адресов>

Указание группы адресов для проверки соответствия адреса получателя сетевого пакета правилу преобразования сетевых адресов (NAT).

Синтаксис

```
set service nat ipv4 rule <номер_правила> destination address-group <имя_группы_адресов>
```

```
delete set service nat ipv4 rule <номер_правила> destination address-group <имя_группы_адресов>
```

```
show set service nat ipv4 rule <номер_правила> destination address-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    nat {
        ipv4 {
            rule номер_правила {
                destination {
                    address-group имя_группы_адресов
                }
            }
        }
    }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

имя_группы_адресов

Проверка соответствия IP-адреса получателя сетевого пакета на основе адресов, входящих в указанную группу. Может быть указана только одна группа адресов. Группа адресов должна быть заранее определена.

Таблица 133 – Допустимые значения для группы адресов

Значение	Описание
<text>	Имя группы
!<text>	Все группы, кроме указанной

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет использовать заранее определенные группы, для указания получателя. Соответствие для пакета устанавливается в том случае, если адрес совпадает с одним из адресов, входящих в состав указанной группы.

ПРИМЕЧАНИЕ Для указания адреса получателя адреса задаются либо указанием группы адресов данной командой, либо указанием отдельного адреса, диапазона адресов или сетей командой service nat ipv4 rule <номер_правила> destination address <адрес>. Параллельное использование обоих механизмов не допускается.

Форма **set** данной команды используется для указания группы адресов получателя для проверки соответствия.

Форма **delete** данной команды используется для удаления группы адресов получателя.

Форма **show** данной команды используется для отображения настройки группы адресов получателя.

18.4.6 service nat ipv4 rule <номер_правила> destination address-type <тип_адреса>

Указание типа адреса получателя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).

Синтаксис

```
set service nat ipv4 rule <номер_правила> destination address-type <тип_адреса>

delete service nat ipv4 rule <номер_правила> destination address-type <тип_адреса>

show service nat ipv4 rule <номер_правила> destination address-type
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    nat {
        ipv4 {
            rule номер_правила {
                destination {
                    address-type тип_адреса
                }
            }
        }
    }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

тип_адреса

Тип адреса получателя (назначения). Допустимые значения приведены в таблице ниже.

Таблица 134 - Допустимые значения типа адреса получателя

Значение	Описание
unspec	Неопределённый адрес (0.0.0.0)
unicast	Однонаправленный адрес
local	Локальный адрес
broadcast	Широковещательный адрес
multicast	Мультивещательный адрес
anycast	Близковещательный адрес (anycast)
blackhole	Адрес подпадающий под маршрут типа "чёрная дыра"
unreachable	Недостижимый адрес
prohibit	Административно запрещённый для маршрутизации адрес
nat	Преобразуемый сетевой адрес

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** используется для создания настройки типа адреса получателя для правила преобразования сетевых адресов (NAT).

Форма **delete** данной команды используется для удаления настройки типа адреса получателя для правила преобразования сетевых адресов (NAT).

Форма **show** данной команды используется для отображения заданного значения типа адреса получателя.

18.4.7 service nat ipv4 rule <номер_правила> destination country <код_страны>

Указание двухзначного кода страны получателя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).

Синтаксис

```
set service nat ipv4 rule <номер_правила> destination country <код_страны>
delete service nat ipv4 rule <номер_правила> destination country <код_страны>
show service nat ipv4 rule <номер_правила> destination country
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    nat {
        ipv4 {
            rule номер_правила {
                destination {
                    country код_страны
                }
            }
        }
    }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

код_страны

Двузначный код страны получателя.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания двухзначного кода страны получателя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).

Форма **set** этой команды используется для указания двухзначного кода страны получателя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).

Форма **delete** этой команды используется для удаления настройки двухзначного кода страны получателя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).

Форма **show** этой команды используется для просмотра настройки двухзначного кода страны получателя.

ПРИМЕЧАНИЕ В одном правиле могут быть заданы не более 15 стран.

18.4.8 service nat ipv4 rule <номер_правила> destination domain-group <имя_группы_доменов>

Указание группы доменов для проверки соответствия адреса получателя сетевого пакета правилу преобразования сетевых адресов (NAT).

Синтаксис

```
set service nat ipv4 rule <номер_правила> destination domain-group <имя_группы_доменов>
delete set service nat ipv4 rule <номер_правила> destination domain-group <имя_группы_доменов>
show set service nat ipv4 rule <номер_правила> destination domain-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    nat {
        ipv4 {
            rule номер_правила {
                destination {
                    domain-group имя_группы_доменов
                }
            }
        }
    }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

имя_группы_доменов

Проверка соответствия домена получателя сетевого пакета на основе доменов, входящих в указанную группу доменов. Соответствие для пакета устанавливается, в том случае если домен получателя совпадает с одним из доменов, входящих в группу. Может быть указана только одна группа доменов. Группа доменов должна быть заранее определена.

Таблица 135 – Допустимые значения для группы доменов

Значение	Описание
<text>	Имя группы
!<text>	Все группы, кроме указанной

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет использовать заранее определенные группы, для указания получателя. Соответствие для пакета устанавливается в том случае, если домен совпадает с одним из доменов, входящих в состав указанной группы.

Форма **set** данной команды используется для указания группы доменов получателя для проверки соответствия.

Форма **delete** данной команды используется для удаления группы доменов получателя.

Форма **show** данной команды используется для отображения настройки группы доменов получателя.

18.4.9 service nat ipv4 rule <номер_правила> destination network-group <имя_группы_сетей>

Данный узел команд присутствует в системе для обеспечения обратной совместимости со старыми версиями оборудования. Вместо него следует использовать функционал service nat ipv4 rule <номер_правила> destination address-group <имя_группы_адресов>. Данный узел может быть удален с дальнейшими обновлениями.

18.4.10 service nat ipv4 rule <номер_правила> destination port-group <имя_группы_портов>

Указание группы сетевых портов для проверки соответствия адреса получателя сетевого пакета правилу преобразования сетевых адресов (NAT).

Синтаксис

```
set service nat ipv4 rule <номер_правила> destination port-group <имя_группы_портов>
```

```
delete set service nat ipv4 rule <номер_правила> destination port-group <имя_группы_портов>
```

```
show set service nat ipv4 rule <номер_правила> destination group port-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    nat {
```

```
        ipv4 {
            rule номер_правила {
                destination {
                    port-group имя_группы_портов
                }
            }
        }
    }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

имя_группы_портов

Проверка соответствия порта получателя сетевого пакета на основе портов, входящих в указанную группу портов. Соответствие для пакета устанавливается в том случае, если порт совпадает с одним из портов, входящих в группу. Может быть указана только одна группа портов. Группа портов должна быть заранее определена.

Таблица 136 – Допустимые значения для группы портов

Значение	Описание
<text>	Имя группы
!<text>	Все группы, кроме указанной

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет использовать заранее определенные группы портов, для указания получателя. Соответствие для пакета устанавливается в том случае, если порт совпадает с одним портов, входящих в состав указанной группы.

ПРИМЕЧАНИЕ Для указания порта получателя порт задается либо указанием группы портов данной командой, либо указанием порта командой service nat ipv4 rule <номер_правила> destination port <порт>. Параллельное использование обоих механизмов не допускается.

Форма **set** данной команды используется для указания группы портов получателя для проверки соответствия.

Форма **delete** данной команды используется для удаления группы портов получателя.

Форма **show** данной команды используется для отображения настройки группы портов получателя.

18.4.11 service nat ipv4 rule <номер_правила> destination port <порт>

Указание номера порта получателя, которые будут использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).

Синтаксис

```
set service nat ipv4 rule <номер_правила> destination port <порт>
delete service nat ipv4 rule <номер_правила> destination port
show service nat ipv4 rule <номер_правила> destination port
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    nat {
        ipv4 {
            rule номер_порта {
                destination {
                    port порт
                }
            }
        }
    }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

порт

Порт получателя для проверки соответствия. Допустимые значения представлены в таблице ниже:

Таблица 137 – Формат указания порта получателя

Значение	Описание
<text>	Имя порта (любое из файла /etc/services)
<0-65535>	Номер порта
<start>-<end>	Диапазон портов

Возможно также задание списка через запятую, например: "22,telnet,http,123,1001-1005".

Возможно также задание инвертированного списка с помощью "!", например: "!22,telnet,http,123,1001-1005".

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания порта получателя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).

ПРИМЕЧАНИЕ Для указания порта получателя порт задается либо указанием порта данной командой, либо указанием группы портов командой service nat ipv4 rule <номер_правила> destination port-group <имя_группы_портов>. Параллельное использование обоих механизмов не допускается.

Форма **set** данной команды позволяет указать порт получателя, используемый при преобразовании сетевых адресов.

Форма **delete** данной команды используется для удаления настройки порта получателя NAT.

Форма **show** данной команды используется для отображения настройки порта получателя NAT.

18.4.12 service nat ipv4 rule <номер_правила> disable

Отключение правила преобразования сетевых адресов (NAT).

Синтаксис

```
set service nat ipv4 rule <номер_правила> disable
delete service nat ipv4 rule <номер_правила> disable
```

```
show service nat ipv4 rule <номер_правила>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    nat {
        ipv4 {
            rule номер_правила {
                disable
            }
        }
    }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

Значение по умолчанию

Правило включено (используется).

Указания по использованию

Команда используется для отключения правила NAT.

Форма **set** данной команды используется для отключения правила NAT.

Форма **delete** данной команды используется для восстановления правила в исходное включенное состояние.

Форма **show** данной команды используется для отображения настройки.

18.4.13 service nat ipv4 rule <номер_правила> exclude

Создание правила, определяющего исключения для указанных пакетов, при преобразовании сетевых адресов.

Синтаксис

```
set service nat ipv4 rule <номер_правила> exclude
delete service nat ipv4 rule <номер_правила> exclude
show service nat ipv4 rule <номер_правила>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    nat {
        ipv4 {
            rule номер_правила  {
                exclude
            }
        }
```

```
    }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать сетевые пакеты, для которых не будет выполняться преобразование сетевых адресов. "Исключающие" правила могут быть полезны в тех случаях, когда для определенных видов трафика (например, для трафика VPN) требуется не выполнять преобразование адресов.

Форма **set** данной команды используется для определения сетевых пакетов, для которых не будет выполняться преобразование сетевых адресов.

Форма **delete** данной команды используется для удаления настройки

Форма **show** данной команды используется для отображения настройки.

18.4.14 service nat ipv4 rule <номер_правила> inbound-interface <интерфейс>

Указание входного интерфейса, на котором будет выполняться правило преобразования сетевого адреса получателя (DNAT).

Синтаксис

```
set service nat ipv4 rule <номер_правила> inbound-interface <интерфейс>
delete service nat ipv4 rule <номер_правила> inbound-interface
show service nat ipv4 rule <номер_правила> inbound-interface
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    nat {
        ipv4 {
            rule номер_правила {
                inbound-interface интерфейс
            }
        }
    }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

интерфейс

Входной интерфейс для выполнения преобразования адресов. Интерфейс должен быть заранее настроен в системе. Также можно указать ключевое слово 'any' для указания любого интерфейса.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания входного интерфейса, на котором будет приниматься трафик для преобразования адресов получателя (DNAT). Преобразование сетевого адреса получателя (DNAT) будет осуществляться для трафика, принятого на указанном интерфейсе.

Данную команду можно использовать только для правил преобразования сетевого адреса получателя (DNAT) (тип destination). Эта команда не может быть использована для правил преобразования сетевых адресов отправителя или правил "маскировки" (виды правил source или masquerade).

Форма **set** данной команды используется для указания входного интерфейса.

Форма **delete** данной команды используется для удаления настройки входного интерфейса.

Форма **show** данной команды используется для отображения настройки входного интерфейса.

18.4.15 service nat ipv4 rule <номер_правила> inside-address address <адрес>

Определение внутреннего адреса для правила, осуществляющего преобразование сетевого адреса получателя.

Синтаксис

```
set service nat ipv4 rule <номер_правила> inside-address address <адрес>
delete service nat ipv4 rule <номер_правила> inside-address address
show service nat ipv4 rule <номер_правила> inside-address address
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   nat {
      ipv4 {
         rule номер_правила {
            inside-address {
               address адрес
            }
         }
      }
   }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

адрес

IPv4-адрес, диапазон адресов, или адрес сети, который используется для преобразования внутреннего адреса. Допустимые форматы указаны в таблице ниже.

Таблица 138 – Формат указания внутреннего адреса

Значение	Описание
x.x.x.x	Преобразование для указанного IPv4-адреса.
x.x.x.x/x	Преобразование для указанной подсети адресов IPv4, адрес узла в подсети останется неизменным.

<x.x.x.x>-<x.x.x.x>	Преобразование для указанного диапазона IPv4-адресов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для указания внутреннего адреса для правила, осуществляющего преобразование сетевого адреса получателя (DNAT).

Указание внутреннего адреса является обязательным для правил преобразования адреса получателя (тип destination). Внутренний адрес не указывается для правил преобразования сетевого адреса отправителя (тип source) или правил "маскировки" (тип masquerade). Правила преобразования сетевого адреса получателя применяются на входе из недоверенной сети в доверенную. Внутренний адрес определяет IP-адрес узла в доверенной сети.

Это адрес, на который будет заменен исходный (первоначальный) IP-адрес получателя сетевого пакета.

Форма **set** данной команды используется для создания и изменения настройки внутреннего адреса для правила, осуществляющего преобразование сетевого адреса получателя (DNAT).

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

18.4.16 service nat ipv4 rule <номер_правила> inside-address port <порт>

Определение внутреннего порта для правила, осуществляющего преобразование сетевого адреса получателя.

Синтаксис

```
set service nat ipv4 rule <номер_правила> inside-address  port <порт>
delete service nat ipv4 rule <номер_правила> inside-address port
show service nat ipv4 rule <номер_правила> inside-address port
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    nat {
        ipv4 {
            rule номер_правила {
                inside-address {
                    port порт
                }
            }
        }
    }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

порт

Порт для преобразования внутреннего адреса. Допустимые значения представлены в таблице ниже:

Таблица 139 – Формат указания порта

Значение	Описание
<text>	Имя порта (любое из файла /etc/services)
<0-65535>	Номер порта
<start>-<end>	Диапазон портов

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для указания внутреннего порта для правила, осуществляющего преобразование сетевого адреса получателя (DNAT).

Указание внутреннего порта является необязательным для правил преобразования адреса получателя (тип destination). Внутренний порт не указывается для правил преобразования сетевого адреса отправителя (тип source) или правил "маскировки" (тип masquerade). Правила преобразования сетевого адреса получателя применяются на входе из недоверенной сети в доверенную. Внутренний порт определяет порт узла в доверенной сети, на который будет перенаправлен трафик.

Это порт, на который будет заменен исходный (первоначальный) порт получателя сетевого пакета.

Форма **set** данной команды используется для создания и изменения настройки внутреннего порта для правила, осуществляющего преобразование сетевого адреса получателя (DNAT).

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

18.4.17 service nat ipv4 rule <номер_правила> log <состояние>

Регистрация для правил преобразования сетевого адреса (NAT), для которых было установлено соответствие.

Синтаксис

```
set service nat ipv4 rule <номер_правила> log <состояние>
delete service nat ipv4 rule <номер_правила> log
show service nat ipv4 rule <номер_правила> log
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    nat {
        ipv4 {
            rule номер_правила {
                log состояние
            }
        }
    }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

состояние

Указание создавать записи журнала для правил преобразования сетевых адресов, для которых было установлено соответствие. Допустимые значения:

enable: Записи журнала для правил, для которых найдено соответствие, создаются.

disable: Записи журнала для правил, для которых найдено соответствие, не создаются.

Значение по умолчанию

Записи журнала для правил, для которых найдено соответствие, не создаются.

Указания по использованию

Данная команда используется для включения и отключения создания записей системного журнала при нахождении соответствия для правила преобразования сетевых адресов. При включении данной функции следует действовать внимательно, так как могут быть созданы файлы журнала очень большого размера, которые могут занять все доступное место на диске.

Форма **set** данной команды используется для установки состояния регистрации.

Форма **delete** данной команды используется для восстановления настройки регистрации для преобразования сетевых адресов в состояние, принятое по умолчанию.

Форма **show** данной команды используется для отображения настройки регистрации для правил преобразования сетевых адресов.

18.4.18 service nat ipv4 rule <номер_правила> outbound-interface <интерфейс>

Указание интерфейса, на который будет передаваться исходящий трафик для правил преобразования адресов отправителя (SNAT) и правил "маскировки" (masquerade).

Синтаксис

```
set service nat ipv4 rule <номер_правила> outbound-interface <интерфейс>
delete service nat ipv4 rule <номер_правила> outbound-interface
show service nat ipv4 rule <номер_правила> outbound-interface
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    nat {
        ipv4 {
            rule номер_правила {
                outbound-interface интерфейс
            }
        }
    }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

интерфейс

Выходной интерфейс для выполнения преобразования адресов. Интерфейс должен быть заранее настроен в системе. Также можно указать ключевое слово 'any' для указания любого интерфейса.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания выходного интерфейса, на котором будет осуществляться преобразование сетевого адреса отправителя (SNAT) или правила "маскировки". Преобразование сетевого адреса отправителя или "маскировка" будет осуществляться для сетевого трафика, передаваемого через данный интерфейс.

Данную команду можно использовать только для правил преобразования сетевого адреса отправителя (SNAT) (тип source) и для правил "маскировки" (тип masquerade) . Эта команда не может быть использована для правил преобразования сетевых адресов получателя (DNAT) (тип destination).

Форма **set** данной команды используется для указания выходного интерфейса.

Форма **delete** данной команды используется для удаления настройки выходного интерфейса.

Форма **show** данной команды используется для отображения настройки выходного интерфейса.

18.4.19 service nat ipv4 rule <номер_правила> outside-address address <адрес>

Определение внешнего адреса для правила преобразования сетевого адреса отправителя (SNAT).

Синтаксис

```
set service nat ipv4 rule <номер_правила> outside-address address <адрес>
delete service nat ipv4 rule <номер_правила> outside-address address
show service nat ipv4 rule ,номер_правила> outside-address address
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   nat {
      ipv4 {
         rule номер_правила {
            outside-address {
               address адрес
            }
         }
      }
   }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

адрес

IPv4-адрес, диапазон адресов, или адрес сети, который используется для преобразования внешнего адреса. Допустимые форматы указаны в таблице ниже.

Таблица 140 – Формат указания внешнего адреса

Значение	Описание
<x.x.x.x>	Преобразование для указанного IPv4-адреса.
<x.x.x.x/x>	Преобразование для указанной подсети адресов IPv4, адрес узла в подсети останется неизменным.
<x.x.x.x>-<x.x.x.x>	Преобразование для указанного диапазона IPv4-адресов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет установить "внешний" IP-адрес для правила преобразования сетевого адреса отправителя. Указание внешнего адреса является обязательным для правил преобразования сетевого адреса отправителя (тип source).

Внешний адрес не может быть указан для правил преобразования сетевого адреса получателя (тип destination) или правил "маскировки" (тип masquerade); для правил "маскировки" (тип masquerade), всегда используется основной адрес интерфейса.

Форма **set** данной команды используется для создания настройки внешнего адреса для правила преобразования сетевого адреса отправителя (SNAT).

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

18.4.20 service nat ipv4 rule <номер_правила> outside-address <порт>

Определение внешнего адреса для правила преобразования сетевого адреса отправителя (SNAT).

Синтаксис

```
set service nat ipv4 rule <номер_правила> outside-address port <порт>
delete service nat ipv4 rule <номер_правила> outside-address port
show service nat ipv4 rule <номер_правила> outside-address port
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   nat {
      ipv4 {
         rule номер_правила {
            outside-address {
               port порт
            }
         }
      }
   }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно нахордиться в диапазоне от 1 до 9999.

порт

Порт для преобразования внешнего адреса. Допустимые значения представлены в таблице ниже:

Таблица 141 – Формат указания порта

Значение	Описание
<text>	Имя порта (любое из файла /etc/services)
<0-65535>	Номер порта

<start>-<end>	Диапазон портов

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет установить "внешний" порт для правила преобразования сетевого адреса отправителя. Указание внешнего порта не является обязательным для правил преобразования сетевого адреса отправителя (тип source).

Форма **set** данной команды используется для создания настройки внешнего порта для правила преобразования сетевого адреса отправителя (SNAT).

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

18.4.21 service nat ipv4 rule <номер_правила> protocol <протокол>

Указание протоколов, для которых осуществляется преобразование сетевых адресов (NAT).

Синтаксис

```
set service nat ipv4 rule <номер_правила> protocol <протокол>
delete service nat ipv4 rule <номер_правила> protocol
show service nat ipv4 rule <номер_правила> protocol
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   nat {
      ipv4 {
         rule номер_правила {
            protocol протокол
         }
      }
   }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

протокол

Сетевой протокол (протоколы), для которого осуществляется преобразование сетевых адресов. Допустимые значения представлены в таблице ниже.

Таблица 142 – Формат указания сетевых протоколов

Значение	Описание
<text>	Имя протокола IP из файла /etc/protocols.
<0-255>	Номер протокола IP.
tcp_upd	Протоколы TCP и UDP.
all	Все протоколы IP.
!<0-255>	Все протоколы IP за исключением указанного.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать протоколы, для которых будет осуществляться преобразование сетевых адресов.

Следует с осторожностью включать в набор правил более одного правила, определяющего исключения (правило, в котором указывается восклицательный знак "!") Правила NAT выполняются по порядку, и последовательность правил, определяющих исключения, может привести к результатам, отличным от ожидаемых.

Форма **set** данной команды позволяет указать протоколы, для которых будет осуществляться преобразование сетевых адресов (NAT).

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

18.4.22 service nat ipv4 rule <номер_правила> source adress <адрес>

Указание адреса отправителя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).

Синтаксис

```
set service nat ipv4 rule <номер_правила> source address  <адрес>
delete service nat ipv4 rule <номер_правила> source address
show service nat ipv4 rule <номер_правила> source address
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   nat {
      ipv4 {
         rule номер_правила {
            source {
               address адрес
            }
         }
      }
   }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

адрес

IPv4-адрес отправителя для проверки соответствия. Допустимые форматы представлены в таблице ниже.

Таблица 143 – Форматы указания адреса отправителя.

Значение	Описание
<x.x.x.x>	IPv4-адрес.

<x.x.x.x/x>	Подсеть адресов IPv4, где 0.0.0.0/0 соответствует любой сети.
<x.x.x.x>-<x.x.x.x>	Диапазон IPv4-адресов.
!<x.x.x.x>	Любой IPv4-адрес, КРОМЕ указанного.
!<x.x.x.x/x>	Любая подсеть адресов IPv4, КРОМЕ указанной подсети.
!<x.x.x.x>-<x.x.x.x>	Любые IPv4-адреса, КРОМЕ лежащих в указанном диапазоне.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда позволяет указать отправителя, на основе которого будет осуществляться Установка соответствия в правиле NAT. Следует с осторожностью включать в набор правил более одного правила, определяющего исключения (правило, в котором указывается восклицательный знак "!"). Правила NAT выполняются по порядку, при этом последовательность правил, определяющих исключения, может привести к результатам, отличным от ожидаемых.

ПРИМЕЧАНИЕ Для указания адреса отправителя адреса задаются либо указанием отдельного адреса, диапазона адресов или сетей данной командой, либо указанием группы адресов командой service nat ipv4 rule <номер_правила> source address-group <имя_группы_адресов>. Параллельное использование обоих механизмов не допускается.

Форма **set** данной команды позволяет указать адрес отправителя, используемый при преобразовании сетевых адресов.

Форма **delete** данной команды используется для удаления настройки адреса отправителя NAT.

Форма **show** данной команды используется для отображения настройки адреса отправителя NAT.

18.4.23 service nat ipv4 rule <номер_правила> source address-group <имя_группы_адресов>

Указание группы адресов для проверки соответствия адреса отправителя сетевого пакета правилу преобразования сетевых адресов (NAT).

Синтаксис

```
set service nat ipv4 rule <номер_правила> source address-group <имя_группы_адресов>
delete set service nat ipv4 rule <номер_правила> source address-group <имя_группы_адресов>
show set service nat ipv4 rule <номер_правила> source address-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    nat {
        ipv4 {
            rule номер_правила {
                source {
                    address-group имя_группы_адресов
                }
            }
        }
    }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

имя_группы_адресов

Проверка соответствия IP-адреса отправителя сетевого пакета на основе адресов, входящих в указанную группу. Может быть указана только одна группа адресов. Группа адресов должна быть заранее определена.

Таблица 144 – Допустимые значения для группы адресов

Значение	Описание
<text>	Имя группы
!<text>	Все группы, кроме указанной

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет использовать заранее определенные группы, для указания отправителя. Соответствие для пакета устанавливается в том случае, если адрес отправителя совпадает с одним из адресов, входящих в состав указанной группы.

ПРИМЕЧАНИЕ Для указания адреса отправителя адреса задаются либо указанием группы адресов данной командой, либо указанием отдельного адреса, диапазона адресов или сетей командой service nat ipv4 rule <номер_правила> source address <адрес>. Параллельное использование обоих механизмов не допускается.

Форма **set** данной команды используется для указания группы адресов отправителя для проверки соответствия.

Форма **delete** данной команды используется для удаления группы адресов отправителя.

Форма **show** данной команды используется для отображения настройки группы адресов отправителя.

18.4.24 service nat ipv4 rule <номер_правила> source address-type <тип_адреса>

Указание типа адреса отправителя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).

Синтаксис

```
set service nat ipv4 rule <номер_правила> source address-type <тип_адреса>
delete service nat ipv4 rule <номер_правила> source address-type <тип_адреса>
show service nat ipv4 rule <номер_правила> source address-type
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    nat {
        ipv4 {
            rule номер_правила {
                source {
                    address-type тип_адреса
                }
            }
```

```
        }
    }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

тип_адреса

Тип адреса отправителя (источника). Допустимые значения приведены в таблице ниже.

Таблица 145 - Допустимые значения типа адреса отправителя

Значение	Описание
unspec	Неопределённый адрес (0.0.0.0)
unicast	Однонаправленный адрес
local	Локальный адрес
broadcast	Широковещательный адрес
multicast	Мультивещательный адрес
anycast	Близковещательный адрес (anycast)
blackhole	Адрес подпадающий под маршрут типа "чёрная дыра"
unreachable	Недостижимый адрес
prohibit	Административно запрещённый для маршрутизации адрес
nat	Преобразуемый сетевой адрес

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** используется для создания настройки типа адреса отправителя для правила преобразования сетевых адресов (NAT).

Форма **delete** данной команды используется для удаления настройки типа адреса отправителя для правила преобразования сетевых адресов (NAT).

Форма **show** данной команды используется для отображения заданного значения типа адреса отправителя.

18.4.25 service nat ipv4 rule <номер_правила> source country <код_страны>

Указание двухзначного кода страны отправителя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).

Синтаксис

```
set service nat ipv4 rule <номер_правила> source country <код_страны>
delete service nat ipv4 rule <номер_правила> source country <код_страны>
show service nat ipv4 rule <номер_правила> source country
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    nat {
        ipv4 {
            rule номер_правила {
                source {
```

```
                country код_страны
            }
        }
    }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

код_страны

Двузначный код страны отправителя.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания двухзначного кода страны отправителя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).

Форма **set** этой команды используется для указания двухзначного кода страны отправителя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).

Форма **delete** этой команды используется для удаления настройки двухзначного кода страны отправителя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).

Форма **show** этой команды используется для просмотра настройки двухзначного кода страны отправителя.

ПРИМЕЧАНИЕ В одном правиле могут быть заданы не более 15 стран.

18.4.26 service nat ipv4 rule <номер_правила> source domain-group <имя_группы_доменов>

Указание группы доменов для проверки соответствия адреса отправителя сетевого пакета правилу преобразования сетевых адресов (NAT).

Синтаксис

```
set service nat ipv4 rule <номер_правила> source domain-group <имя_группы_доменов>
delete set service nat ipv4 rule <номер_правила> source domain-group <имя_группы_доменов>
show set service nat ipv4 rule <номер_правила> source domain-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    nat {
        ipv4 {
            rule номер_правила {
                source {
                    address-group имя_группы_доменов
```

```
                }
            }
        }
    }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

имя_группы_доменов

Проверка соответствия домена отправителя сетевого пакета на основе доменов, входящих в указанную группу доменов. Соответствие для пакета устанавливается, в том случае если домен отправителя совпадает с одним из доменов, входящих в группу. Может быть указана только одна группа доменов. Группа доменов должна быть заранее определена.

Таблица 146 – Допустимые значения для группы доменов

Значение	Описание
<text>	Имя группы
!<text>	Все группы, кроме указанной

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет использовать заранее определенные группы, для указания отправителя. Соответствие для пакета устанавливается в том случае, если домен совпадает с одним из доменов, входящих в состав указанной группы.

Форма **set** данной команды используется для указания группы доменов отправителя для проверки соответствия.

Форма **delete** данной команды используется для удаления группы доменов отправителя.

Форма **show** данной команды используется для отображения настройки группы доменов отправителя.

18.4.27 service nat ipv4 rule <номер_правила> source network-group <имя_группы_сетей>

Данный узел команд присутствует в системе для обеспечения обратной совместимости со старыми версиями оборудования. Вместо него следует использовать функционал **service nat ipv4 rule <номер_правила> source address-group <имя_группы_адресов>**.

18.4.28 service nat ipv4 rule <номер_правила> source port-group <имя_группы_портов>

Указание группы сетевых портов для проверки соответствия адреса отправителя сетевого пакета правилу преобразования сетевых адресов (NAT).

Синтаксис

```
set service nat ipv4 rule <номер_правила> source port-group
<имя_группы_портов>

delete set service nat ipv4 rule <номер_правила> source port-group
<имя_группы_портов>

show set service nat ipv4 rule <номер_правила> source group port-group
<имя_группы_портов>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    nat {
        ipv4 {
            rule номер_правила {
                source {
                    address-group имя_группы_портов
                }
            }
        }
    }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

имя_группы_портов

Проверка соответствия порта отправителя сетевого пакета на основе портов, входящих в указанную группу портов. Соответствие для пакета устанавливается в том случае, если порт отправителя совпадает с одним из портов, входящих в группу. Может быть указана только одна группа портов. Группа портов должна быть заранее определена.

Таблица 147 – Допустимые значения для группы портов

Значение	Описание
<text>	Имя группы
!<text>	Все группы, кроме указанной

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет использовать заранее определенные группы портов, для указания отправителя. Соответствие для пакета устанавливается в том случае, если порт совпадает с одним портов, входящих в состав указанной группы.

ПРИМЕЧАНИЕ Для указания порта отправителя порт задается либо указанием группы портов данной командой, либо указанием порта командой **service nat ipv4 rule <номер_правила> source port <порт>**. Параллельное использование обоих механизмов не допускается.

Форма **set** данной команды используется для указания группы портов отправителя для проверки соответствия.

Форма **delete** данной команды используется для удаления группы портов отправителя.

Форма **show** данной команды используется для отображения настройки группы портов отправителя.

18.4.29 service nat ipv4 rule <номер_правила> source port <порт>

Указание номера порта отправителя, которые будут использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).

Синтаксис

```
set service nat ipv4 rule <номер_правила> source port <порт>
delete service nat ipv4 rule <номер_правила> source port <порт>
show service nat ipv4 rule <номер_правила> source port
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   nat {
      ipv4 {
         rule номер_порта {
            source {
               port порт
            }
         }
      }
   }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

порт

Порт отправителя для проверки соответствия. Допустимые значения представлены в таблице ниже:

Таблица 148 – Формат указания порта отправителя

Значение	Описание
<text>	Имя порта (любое из файла /etc/services)
<0-65535>	Номер порта
<start>-<end>	Диапазон портов

Возможно также задание инвертированного списка с помощью "!", например: "!22,telnet,http,123,1001-1005".

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания порта отправителя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).

ПРИМЕЧАНИЕ Для указания порта отправителя порт задается либо указанием порта данной командой, либо указанием группы портов командой **service nat ipv4 rule <номер_правила> source port-group <имя_группы_портов>**. Параллельное использование обоих механизмов не допускается.

Форма **set** данной команды позволяет указать порт отправителя, используемый при преобразовании сетевых адресов.

Форма **delete** данной команды используется для удаления настройки порта отправителя NAT.

Форма **show** данной команды используется для отображения настройки порта отправителя NAT.

18.4.30 service nat ipv4 rule <номер_правила> type <вид>

Установка вида преобразования для правила преобразования сетевого адреса (NAT).

Синтаксис

```
set service nat ipv4 rule <номер_правила> type <вид>
delete service nat ipv4 rule <номер_правила> type
show service nat ipv4 rule <номер_правила> type
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   nat {
      ipv4 {
         rule номер_правила {
            type вид
         }
      }
   }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

вид

Указывает, какое преобразование адресов выполняется в правиле. Допустимые значения представлены в таблице ниже.

Таблица 149 – Типы преобразования адресов

Значение	Описание
destination	Данное правило используется для преобразования сетевых адресов получателя.
source	Данное правило используется для преобразования сетевых адресов отправителя.
masquerade	Данный вид правил является частным случаем преобразования сетевого адреса отправителя. Преобразование сетевого адреса отправителя осуществляется с использованием IP-адреса внешнего интерфейса маршрутизатора в качестве адреса для замены.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать вид преобразования сетевых адресов.

Необходимо создать отдельное правило преобразования сетевых адресов для каждого направления сетевого трафика. Например, при настройке преобразования сетевого адреса отправителя вида "один к одному" для исходящего трафика необходимо создать отдельное правило.

Правила преобразования сетевого адреса отправителя обычно применяются на выходе из доверенной сети в недоверенную. Для правил преобразования сетевых адресов отправителя внешний адрес обычно определяет IP-адрес, который обращен к недоверенной сети. Это адрес, на который заменяется первоначальный IP-адрес отправителя для исходящих пакетов.

Форма **set** данной команды позволяет определить вид преобразования сетевых адресов (отправителя/получателя).

Форма **delete** данной команды используется для удаления настройки

Форма **show** данной команды используется для отображения настройки.

18.4.31 service nat ethernet

Включение преобразования сетевых адресов (NAT) для протокола ethernet.

Синтаксис

```
set service nat ethernet
delete service nat ethernet
show service nat ethernet
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   nat{
      ethernet {
      }
   }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет включить преобразование сетевых адресов (NAT) для протокола ethernet в системе.

Форма **set** данной команды используется для создания и изменения настройки NAT.

Форма **delete** данной команды используется для удаления настройки NAT и отключения преобразования сетевых адресов в системе.

Форма **show** данной команды используется для отображения настройки NAT.

18.4.32 service nat ethernet rule <номер_правила>

Определение правила преобразования сетевых адресов (NAT) для протокола ethernet.

Синтаксис

```
set service nat ethernet rule <номер_правила>
delete service nat ethernet rule <номер_правила>
show service nat ethernet rule <номер_правила>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   nat {
      ethernet {
         rule номер_правила {
         }
```

```
        }
    }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания настройки правила преобразования сетевых адресов (NAT). Правила NAT исполняются в порядке следования их номеров. Следует отметить, что идентификатор правила NAT (номер правила) не может быть изменен после создания правила. Для обеспечения возможности вставки в будущем дополнительных правил, следует при назначении номеров правил оставлять интервалы; например, установить номера для начального набора правил: 10, 20, 30, 40, и т. д.

Форма **set** данной команды используется для создания и изменения правила NAT.

Форма **delete** данной команды используется для удаления правила NAT.

Форма **show** данной команды используется для отображения настройки правила NAT.

18.4.33 service nat ethernet rule <номер_правила> action <действие> to <mac-адрес>

Указание действия, которое будет применяться к пакетам, для которых было установлено соответствие правилу.

Синтаксис

```
set service nat ethernet rule <номер_правила> action <действие> to <mac-адрес>
delete service nat ethernet rule <номер_правила> action <действие>
show service nat ethernet rule <номер_правила> action <действие>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    nat {
        ethernet {
            rule номер_правила {
                action действие {
                    to mac-адрес
                }
            }
        }
    }
}
```

Параметры

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

действие

Действие, которое следует выполнено при применении данного правила. Допустимые значения представлены в таблице ниже.

Таблица 150 – Допустимые действия для правил NAT ethernet

Значение	Описание
exclude	Исключить. Обязательным параметром является входящий и исходящий интерфейс.
snat	Преобразовать адрес отправителя. Обязательным параметром является исходящий интерфейс.
snat_arp	Преобразовать адрес отправителя и адрес в пакетах ARP. Обязательным параметром является исходящий интерфейс.
dnat	Преобразовать адрес получателя. Обязательным параметром является входящий интерфейс.

mac-адрес

MAC-адрес устройства, на который будет произведена замена.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать действие, которое следует выполнено при применении данного правила.

Форма **set** данной команды используется для указания действия, которое следует выполнено при применении данного правила.

Форма **delete** данной команды позволяет восстановить действие, принятое по умолчанию.

Форма **show** данной команды используется для отображения настройки действия для правила NAT.

18.4.34 service nat ethernet rule <номер_правила> description <описание>

Указание описания правила NAT для протокола ethernet.

Синтаксис

```
set service nat ethernet rule <номер_правила> description <описание>
delete service nat ethernet rule <номер_правила> description
show service nat ethernet rule <номер_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   nat {
      ethernet {
         rule номер_правила {
            description описание
         }
      }
   }
}
```

Параметры

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

описание

Описание правила. В том случае если описание содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать описание для правила NAT.

Форма **set** данной команды используется для создания и изменения описания.

Форма **delete** используется для удаления описания.

Форма **show** используется для отображения настройки описания.

18.4.35 service nat ethernet rule <номер_правила> destination ip <адрес>

Указание ip-адреса получателя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).

Синтаксис

```
set service nat ethernet rule <номер_правила> destination ip <адрес>
delete service nat ethernet rule <номер_правила> destination ip
show service nat ethernet rule <номер_правила> destination ip
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   nat {
      ethernet {
         rule номер_правила {
            destination {
               ip адрес
            }
         }
      }
   }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

адрес

IPv4-адрес получателя для проверки соответствия. Допустимые форматы представлены в таблице ниже.

Таблица 151 – Форматы указания адреса получателя.

Значение	Описание
<x.x.x.x>	IPv4-адрес.
<x.x.x.x/x>	Подсеть адресов IPv4, где 0.0.0.0/0 соответствует любой сети.
!<x.x.x.x>	Любой IPv4-адрес, КРОМЕ указанного.
!<x.x.x.x/x>	Любая подсеть адресов IPv4, КРОМЕ указанной подсети.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда позволяет указать ip-адрес получателя, на основе которого будет осуществляться Установка соответствия в правиле NAT. Следует с осторожностью включать в набор правил более одного правила, определяющего исключения (правило, в котором указывается восклицательный знак "!"). Правила NAT выполняются по порядку, при этом последовательность правил, определяющих исключения, может привести к результатам, отличным от ожидаемых.

Форма **set** данной команды позволяет указать ip-адрес получателя, используемый при преобразовании сетевых адресов.

Форма **delete** данной команды используется для удаления настройки ip-адреса получателя NAT.

Форма **show** данной команды используется для отображения настройки ip-адреса получателя NAT.

18.4.36 service nat ethernet rule <номер_правила> destination mac <mac-адрес>

Указание mac-адреса получателя, который будет использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).

Синтаксис

```
set service nat ethernet rule <номер_правила> destination mac <mac-адрес>
delete service nat ethernet rule <номер_правила> destination mac
show service nat ethernet rule <номер_правила> destination mac
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   nat {
      ethernet {
         rule номер_правила {
            destination {
               mac mac-адрес
            }
         }
      }
   }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

mac-адрес

MAC-адрес получателя для проверки соответствия. Допустимые форматы представлены в таблице ниже.

Таблица 152 – Форматы указания MAC-адреса

Значение	Описание
<h:h:h:h:h:h>	MAC-адрес
!<h:h:h:h:h:h>	Все адреса за исключением указанного
<h:h:h:h:h:h>/<h:h:h:h:h:h>	Множество адресов, задаваемое адресом и маской

!<h:h:h:h:h:h>/<h:h:h:h:h:h>	Все адреса, кроме указанного множества
unicast	соответствует однонаправленным адресам 00:00:00:00:00:00/01:00:00:00:00:00
multicast	соответствует мультивещательным адресам 01:00:00:00:00:00/01:00:00:00:00:00
broadcast	соответствует широковещательному адресу ff:ff:ff:ff:ff:ff
bga	соответствует bridge group адресу 01:80:c2:00:00:00/ff:ff:ff:ff:ff:ff

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда позволяет указать mac-адрес получателя, на основе которого будет осуществляться Установка соответствия в правиле NAT. Следует с осторожностью включать в набор правил более одного правила, определяющего исключения (правило, в котором указывается восклицательный знак "!"). Правила NAT выполняются по порядку, при этом последовательность правил, определяющих исключения, может привести к результатам, отличным от ожидаемых.

Форма **set** данной команды позволяет указать mac-адрес получателя, используемый при преобразовании сетевых адресов.

Форма **delete** данной команды используется для удаления настройки mac-адреса получателя NAT.

Форма **show** данной команды используется для отображения настройки mac-адреса получателя NAT.

18.4.37 service nat ethernet rule <номер_правила> disable

Отключение правила преобразования сетевых адресов (NAT) для протокола ethernet.

Синтаксис

```
set service nat ethernet rule <номер_правила> disable
delete service nat ethernet rule <номер_правила> disable
show service nat ethernet rule <номер_правила>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    nat {
        ethernet {
            rule номер_правила {
                disable
            }
        }
    }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

Значение по умолчанию

Правило включено (используется).

Указания по использованию

Команда используется для отключения правила NAT.

Форма **set** данной команды используется для отключения правила NAT.

Форма **delete** данной команды используется для восстановления правила в исходное включенное состояние.

Форма **show** данной команды используется для отображения настройки.

18.4.38 service nat ethernet rule <номер_правила> interface in <интерфейс>

Указание входного интерфейса, на котором будет выполняться правило преобразования сетевого адреса получателя (DNAT) и интерфейса.

Синтаксис

```
set service nat ethernet rule <номер_правила> interface in <интерфейс>
delete service nat ethernet rule <номер_правила> interface in
show service nat ethernet rule <номер_правила> interface in
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   nat {
      ethernet {
         rule номер_правила {
            interface {
               in интерфейс
            }
         }
      }
   }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

интерфейс

Входной интерфейс для выполнения преобразования адресов. Интерфейс должен быть заранее настроен в системе. Также можно указать ключевое слово 'any' для указания любого интерфейса.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания входного интерфейса, на котором будет выполняться правило преобразования сетевого адреса получателя (DNAT).

Форма **set** данной команды используется для указания входного интерфейса.

Форма **delete** данной команды используется для удаления настройки входного интерфейса.

Форма **show** данной команды используется для отображения настройки входного интерфейса.

18.4.39 service nat ethernet rule <номер_правила> interface out <интерфейс>

Указание исходящего интерфейса, на который будет передаваться исходящий трафик для правил преобразования адресов отправителя (SNAT).

Синтаксис

```
set service nat ethernet rule <номер_правила> interface out <интерфейс>
delete service nat ethernet rule <номер_правила> interface out
show service nat ethernet rule <номер_правила> interface out
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   nat {
      ethernet {
         rule номер_правила {
            interface {
               out интерфейс
            }
         }
      }
   }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

интерфейс

Выходной интерфейс для выполнения преобразования адресов. Интерфейс должен быть заранее настроен в системе. Также можно указать ключевое слово 'any' для указания любого интерфейса.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания исходящего интерфейса, на который будет передаваться исходящий трафик для правил преобразования адресов отправителя (SNAT).

Форма **set** данной команды используется для указания исходящего интерфейса.

Форма **delete** данной команды используется для удаления настройки исходящего интерфейса.

Форма **show** данной команды используется для отображения настройки исходящего интерфейса.

18.4.40 service nat ethernet rule <номер_правила> log <состояние>

Регистрация для правил преобразования сетевого адреса (NAT), для которых было установлено соответствие.

Синтаксис

```
set service nat ethernet rule <номер_правила> log <состояние>
delete service nat ethernet rule <номер_правила> log
show service nat ethernet rule <номер_правила> log
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    nat {
        ethernet {
            rule номер_правила {
                log состояние
            }
        }
    }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

состояние

Указание создавать записи журнала для правил преобразования сетевых адресов, для которых было установлено соответствие. Допустимые значения:

enable: Записи журнала для правил, для которых найдено соответствие, создаются;

disable: Записи журнала для правил, для которых найдено соответствие, не создаются.

Значение по умолчанию

Записи журнала для правил, для которых найдено соответствие, не создаются.

Указания по использованию

Данная команда используется для включения и отключения создания записей системного журнала при нахождении соответствия для правила преобразования сетевых адресов.

При включении данной функции следует действовать внимательно, так как могут быть созданы файлы журнала очень большого размера, которые могут занять все доступное место на диске.

Форма **set** данной команды используется для установки состояния регистрации.

Форма **delete** данной команды используется для восстановления настройки регистрации для преобразования сетевых адресов в состояние, принятое по умолчанию.

Форма **show** данной команды используется для отображения настройки регистрации для правил преобразования сетевых адресов.

18.4.41 service nat ethernet rule <номер_правила> protocol <протокол>

Указание протоколов, для которых осуществляется преобразование сетевых адресов (NAT).

Синтаксис

```
set service nat ethernet rule <номер_правила> protocol <протокол>
delete service nat ethernet rule <номер_правила> protocol
show service nat ethernet rule <номер_правила> protocol
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    nat {
        ethernet {
```

```
            rule номер_правила {
               protocol протокол
            }
         }
      }
   }
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

протокол

Протокол, пакет которого инкапсулирован в Ethernet-кадре. Допустимые форматы значений представлены в таблице ниже.

Таблица 153 – Формат указания протокола

Значение	**Описание**
<600-ffff>	Номер протокола в шестнадцатеричном формате
!<600-ffff>	Все кадры за исключением кадров с указанным протоколом
ipv4	IPv4
x.25	X.25
arp	Address Resolution Protocol
frame-relay-arp	Frame Relay ARP
bpq	G8BPQ AX.25 Ethernet
dec	DEC Assigned protocol
dec-dna-dl	DEC DNA Dump/Load
dec-dna-rc	DEC DNA Remote Console
dec-dna-re	DEC DNA Routing
dec-lat	DEC LAT
dec-diag	DEC Diagnostics
dec-cust	DEC Customer use
dec-sca	DEC Systems Comms Arch
teb	Trans Ether Bridging
frame-relay-raw	Raw Frame Relay
aarp	Appletalk AARP
appletalk	Appletalk DDP
802.1q	802.1Q Virtual LAN tagged frame
ipx	Novell IPX
netbeui	NetBIOS Extended User Interface
ipv6	IPv6
ppp	Point-to-Point Protocol
atm-mpoa	MultiProtocol Over ATM
pppoe-disc	PPPoE discovery messages
pppoe-ses	PPPoE session messages
atm-fate	Frame-based ATM Transport over Ethernet
loop	Ethernet Loopback protocol
length	Номер протокола меньше 0x600 и используется в качестве длины

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать протоколы, для которых будет осуществляться преобразование сетевых адресов. Следует с осторожностью включать в набор правил более одного правила, определяющего исключения (правило, в котором указывается восклицательный знак "!") Правила NAT выполняются по порядку, и последовательность правил, определяющих исключения, может привести к результатам, отличным от ожидаемых.

Форма **set** данной команды позволяет указать протоколы, для которых будет осуществляться преобразование сетевых адресов (NAT).

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

18.4.42 service nat ethernet rule <номер_правила> source ip <адрес>

Указание IP-адреса и MAC-адреса отправителя, по которым будет осуществляться проверка соответствия в правиле преобразования сетевого адреса (NAT) для протокола ethernet.

Синтаксис

```
set service nat ethernet rule <номер_правила> source ip <адрес>
delete service nat ethernet rule <номер_правила> source ip
show service nat ethernet rule <номер_правила> source ip
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   nat {
      ethernet {
         rule номер_правила {
            source {
               ip адрес
            }
         }
      }
   }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

адрес

IPv4-адрес отправителя для проверки соответствия. Допустимые форматы представлены в таблице ниже.

Таблица 154 – Форматы указания адреса получателя.

Значение	Описание
<x.x.x.x>	IPv4-адрес.
<x.x.x.x/x>	Подсеть адресов IPv4, где 0.0.0.0/0 соответствует любой сети.
!<x.x.x.x>	Любой IPv4-адрес, КРОМЕ указанного.

!<x.x.x.x/x>	Любая подсеть адресов IPv4, КРОМЕ указанной подсети.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать ip-адрес отправителя, по которому будет осуществляться проверка соответствия для правила преобразования сетевого адреса. Следует с осторожностью включать в набор правил более одного правила, определяющего исключения (правило, в котором указывается восклицательный знак "!"). Правила NAT выполняются последовательно, и набор правил, содержащий более одного "исключающего" правила, может привести к результатам, отличным от ожидаемых.

Форма **set** данной команды используется для создания ip-адреса отправителя для преобразования сетевых адресов.

Форма **delete** данной команды позволяет удалить настройку ip-адреса отправителя для преобразования сетевых адресов.

Форма **show** данной команды используется для отображения настройки ip-адреса отправителя для преобразования сетевых адресов.

18.4.43 service nat ethernet rule <номер_правила> source mac <mac-адрес>

Указание MAC-адреса отправителя, по которым будет осуществляться проверка соответствия в правиле преобразования сетевого адреса (NAT) для протокола ethernet.

Синтаксис

```
set service nat ethernet rule <номер_правила> source mac <mac-адрес>

delete service nat ipv4 rule <номер_правила> source mac

show service nat ipv4 rule <номер_правила> source mac
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   nat {
      ethernet {
         rule номер_правила {
            source {
               mac mac-адрес
            }
         }
      }
   }
}
```

Параметры

номер_правила

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

mac-адрес

MAC-адрес отправителя для проверки соответствия. Допустимые форматы представлены в таблице ниже.

Таблица 155 – Форматы указания MAC-адреса

Значение	Описание

<h:h:h:h:h:h>	MAC-адрес
!<h:h:h:h:h:h>	Все адреса за исключением указанного
<h:h:h:h:h:h>/<h:h:h:h:h:h>	Множество адресов, задаваемое адресом и маской
!<h:h:h:h:h:h>/<h:h:h:h:h:h>	Все адреса, кроме указанного множества
unicast	соответствует однонаправленным адресам 00:00:00:00:00:00/01:00:00:00:00:00
multicast	соответствует мультивещательным адресам 01:00:00:00:00:00/01:00:00:00:00:00
broadcast	соответствует широковещательному адресу ff:ff:ff:ff:ff:ff
bga	соответствует bridge group адресу 01:80:c2:00:00:00/ff:ff:ff:ff:ff:ff

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать MAC-адрес отправителя, по которому будет осуществляться проверка соответствия для правила преобразования сетевого адреса. Следует с осторожностью включать в набор правил более одного правила, определяющего исключения (правило, в котором указывается восклицательный знак "!"). Правила NAT выполняются последовательно, и набор правил, содержащий более одного "исключающего" правила, может привести к результатам, отличным от ожидаемых.

Форма **set** данной команды используется для создания MAC-адреса отправителя для преобразования сетевых адресов.

Форма **delete** данной команды позволяет удалить настройку MAC-адреса отправителя для преобразования сетевых адресов.

Форма **show** данной команды используется для отображения настройки MAC-адреса отправителя для преобразования сетевых адресов.

18.4.44 clear nat ipv4 counters

Очистка счетчиков для активных IPv4-правил преобразования сетевых адресов (NAT).

Синтаксис

```
clear nat ipv4 counters [rule <номер_правила>]
```

Режим ввода команды

Эксплуатационный режим.

Параметры

номер_правила

Численный идентификатор правила. Значение должно находиться в диапазоне от 1 до 9999.

Значение по умолчанию

Счетчики сбрасываются для всех правил преобразования сетевых адресов (NAT).

Указания по использованию

Команда позволяет сбросить счетчики для IPv4-правил преобразования сетевых адресов (NAT). По умолчанию счетчики сбрасываются для всех правил. Если указывается номер правила, счетчики сбрасываются только для указанного правила.

18.4.45 clear nat ethernet counters

Очистка счетчиков для активных Ethernet-правил преобразования сетевых адресов (NAT).

Синтаксис

```
clear nat ethernet counters
```

Режим ввода команды

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Счетчики сбрасываются для всех правил преобразования сетевых адресов (NAT).

Указания по использованию

Команда позволяет сбросить счетчики для Ethernet-правил преобразования сетевых адресов (NAT).

18.4.46 show nat ipv4 rules

Отображение настроенных правил преобразования сетевых адресов (NAT).

Синтаксис

```
show nat ipv4 rules
```

Режим ввода команды

Эксплуатационный режим.

Параметры

Отсутствуют.

Указания по использованию

Данная команда позволяет отобразить настроенные правила преобразования сетевых адресов. Данная команда может использоваться для выявления неисправностей, а также для проверки того, что соответствие устанавливается для требуемого сетевого трафика.

Пример

В примере ниже приведен вывод для команды show nat ipv4 rules . В данном выводе используются следующие аббревиатуры:

- saddr - адрес отправителя;
- sport- порт отправителя;
- daddr- адрес получателя;
- dport- порт получателя;
- proto- протокол;
- intf- интерфейс.

Также необходимо отметить следующее:

Для указания интерфейса используется только одна колонка intf. Для правил преобразования сетевого адреса отправителя или правил "маскировки" в качестве интерфейса указывается выходной интерфейс; для правил преобразования сетевого адреса получателя в качестве интерфейса указывается входной интерфейс. В колонке преобразования (translation), в первых двух строках выводятся сведения о преобразовании, в третьей строке (в том случае если она представлена) выводятся условия для осуществления преобразования.

Пример 162 – Вывод сведений о правилах NAT

```
admin@edge:~$ show nat ipv4 rules

Type Codes:  SRC - source, DST - destination, MASQ - masquerade
              X at the front of rule implies rule is excluded

rule   type  intf     translation
----   ----  ----     -----------
10     DST   any      daddr 10.0.0.1 to 192.168.0.1
    proto-tcp_udp     dport ANY
```

18.4.47 show nat ipv4 statistics

Вывод статистики для службы преобразования сетевых адресов (NAT).

Синтаксис

```
show nat ipv4 statistics
```

Режим ввода команды

Эксплуатационный режим.

Параметры

Отсутствуют.

Указания по использованию

Данная команда используется для вывода текущей статистики для правил преобразования сетевых адресов.

Примеры

В примере ниже приведен вывод для команды show nat ipv4 statistics. В данном выводе используются следующие аббревиатуры:

- rule - номер правила;
- count- количество пакетов;
- type- тип правила;
- IN- входящий интерфейс;
- OUT- исходящий интерфейс.

Пример 163 – Вывод сведений о статистике для правил NAT

```
admin@edge:~$ show nat ipv4 statistics

Type Codes:  SRC - source, DST - destination, MASQ - masquerade

rule  count     type     IN         OUT
----  -------   ----  ---------  ---------
10    147       DST   any            -
```

18.4.48 show nat ipv4 translations

Вывод сведений о трансляциях сетевых адресов.

Синтаксис

```
show nat ipv4 translations [ detail | monitor [detail]]
```

Режим ввода команды

Эксплуатационный режим.

Параметры

monitor

Показать активные события трансляции адресов (NAT).

detail

Показ подробных сведений.

Указания по использованию

Данная команда позволяет вывести сведения о трансляциях сетевых адресов.

Пример

В примере ниже приведен образец вывода для команды show nat ipv4 translations.

Пример 164 – Вывод преобразований сетевых адресов

```
admin@edge:~$ show nat ipv4 translations
Pre-NAT              Post-NAT            Type    Prot    Timeout
192.168.10.1         192.168.11.254      snat    icmp    29
192.168.11.1         192.168.11.1        dnat    icmp    29
```

18.4.49 show nat ipv4 translations destination

Вывод сведений о трансляциях сетевых адресов получателя (DNAT).

Синтаксис

```
show nat ipv4 translations destination [address <адрес> | detail | monitor [detail]]
```

Режим ввода команды

Эксплуатационный режим.

Параметры

адрес

IPv4-адрес получателя для проверки соответствия.

monitor

Показать активные события трансляции адресов получателя (DNAT).

detail

Показ подробных сведений.

Указания по использованию

Данная команда позволяет вывести сведения о трансляциях сетевых адресов получателя.

Пример

В примере ниже приведен образец вывода для команды show nat ipv4 translations destination address 192.168.10.254.

Пример 165 – Вывод сведений NAT для адреса получателя 192.168.10.254

```
admin@edge:~$ show nat ipv4 translations destination address 192.168.10.254
Pre-NAT src          Pre-NAT dst          Post-NAT src         Post-NAT dst
192.168.10.1         192.168.10.254       192.168.10.1         192.168.11.1

icmp: dnat: 192.168.10.254 ==> 192.168.11.1 timeout: 29 use: 1
```

18.4.50 show nat ipv4 translations source

Вывод сведений о трансляциях сетевых адресов отправителя (SNAT).

Синтаксис

```
show nat ipv4 translations source [address <адрес> | detail | monitor [detail]]
```

Режим ввода команды

Эксплуатационный режим.

Параметры

адрес

IPv4-адрес отправителя для проверки соответствия.

monitor

Показать активные события трансляции адресов отправителя (SNAT).

detail

Показ подробных сведений.

Указания по использованию

Данная команда позволяет вывести сведения о трансляциях сетевых адресов отправителя.

Пример

В примере ниже приведен образец вывода для команды show nat ipv4 translations source address 192.168.10.1.

Пример 166 – Вывод сведений NAT для адреса отправителя 192.168.10.1

```
admin@edge:~$ show nat ipv4 translations source address 192.168.10.1
Pre-NAT src          Pre-NAT dst          Post-NAT src         Post-NAT dst
192.168.10.1         192.168.11.1         192.168.11.254       192.168.11.1

icmp: snat: 192.168.10.1 ==> 192.168.11.254 timeout: 29 use: 1
```

18.4.51 show nat ethernet rules

Отображение настроенных правил преобразования сетевых адресов (NAT) для протокола ethernet.

Синтаксис

```
show nat ethernet rules
```

Режим ввода команды

Эксплуатационный режим.

Параметры

Отсутствуют.

Указания по использованию

Данная команда позволяет отобразить настроенные правила преобразования сетевых адресов. Данная команда может использоваться для выявления неисправностей, а также для проверки того, что соответствие устанавливается для требуемого сетевого трафика.

Пример

В примере ниже приведен вывод для команды show nat ipv4 rules . В данном выводе используются следующие аббревиатуры:

- src IP - адрес отправителя;
- src MAC- mac отправителя;
- dst IP- адрес получателя;
- dport- порт получателя;
- proto- протокол;
- rule- номер правила;
- type- тип трансляции;
- iface in- входящий интерфейс;
- iface out- исходящий интерфейс;
- translation- правило преобразования.

Также необходимо отметить следующее:

Для правил преобразования сетевого адреса отправителя или правил "маскировки" в качестве интерфейса указывается выходной интерфейс; для правил преобразования сетевого адреса получателя в качестве интерфейса указывается входной интерфейс.

В колонке преобразования (translation), в первых двух строках выводятся сведения о преобразовании, в третьей строке (в том случае если она представлена) выводятся условия для осуществления преобразования. Например, правило 10, которое является правилом преобразования сетевого адреса отправителя (SNAT), заменяет адреса отправителя 192.168.74.0/24 на адреса 172.16.139.0/24 и изменяет MAC-адрес отправителя на "11:22:33:44:55:66".

Если перед номером правила указывается символ "X", правило является исключающим.

Пример 167 – Вывод сведений о правилах NAT

```
admin@edge# run show nat ethernet rules

rule    type    iface in    iface out   translation
----    ----    --------    ---------   -----------
10      SNAT    -           eth1        src MAC unicast to 11:22:33:44:55:66
   src MAC unicast src IP 192.168.10.0/24 dst IP 192.168.11.0/24 proto ipv4
```

18.4.52 show nat ethernet statistics

Вывод статистики для службы преобразования сетевых адресов (NAT) для протокола ethernet.

Синтаксис

```
show nat ethernet statistics
```

Режим ввода команды

Эксплуатационный режим.

Параметры

Отсутствуют.

Указания по использованию

Данная команда используется для вывода текущей статистики для правил преобразования сетевых адресов.

Примеры

В примере ниже приведен вывод для команды show nat ipv4 statistics. В данном выводе используются следующие аббревиатуры:

- rule - номер правила;
- count- количество пакетов;
- type- тип правила;
- IN- входящий интерфейс;
- OUT- исходящий интерфейс;

Пример 168 – Вывод сведений о статистике для правил NAT

```
admin@edge# run show nat ethernet statistics

rule    pkts    type    iface in    iface out
----    ----    ----    --------    ---------
10      0       SNAT    -           eth1
```

19 Фильтрация по классификационным (мандатным) меткам в сетевом трафике

19.1 Обзор механизмов фильтрации по классификационным меткам

В этом разделе рассматриваются возможности по фильтрации сетевого трафика, содержащего в себе классификационные (мандатные) метки, в частности рассматриваются:

- поддерживаемые стандарты;
- обзор структуры классификационной метки в сетевом трафике.

19.1.1 Поддерживаемые стандарты

Numa Edge реализует фильтрацию сетевого трафика, содержащего классификационные (мандатные) метки, соответствующие описанию приведенному в RFC 1108 «U.S. Department of Defense Security Options for the Internet Protocol».

19.1.2 Обзор структуры классификационной метки в сетевом трафике

Согласно RFC 1108 при передаче информации по протоколу IPv4 классификационные метки размещаются в каждом заголовке IP-пакета в поле Опции (Options) с типом Безопасность (Security). При этом используется следующий формат:

Таблица 156 – Описание полей, входящих в поле опция

Поля, входящие в поле Опции	**Значение**
TYPE (8 бит)	10000010 (130 в десятичном представлении, что определяет тип поля Опции — Безопасность (Security))
LENGTH (8 бит)	Значение длины поля Опции в октетах.
CLASSIFICATION LEVEL (8 бит)	Указывается уровень конфиденциальности (степень секретности).
PROTECTION AUTHORITY FLAGS (переменной длинны)	Указывается принадлежность (подведомственность) трафика определенному органу по защите, определяющему правила защиты для передачи и обработки информации, содержащейся в информационном потоке.

19.2 Пример настройки фильтрации по классификационным меткам

В этом разделе рассматриваются пример конфигурации Numa Edge осуществляющей фильтрацию по классификационным меткам в сетевом трафике. В пределах стенда необходимо обеспечить возможность прохождения от АРМ №1 к Сервер №1 исключительно сетевого трафика содержащего классификационные метки соответствующие уровням конфиденциальности 1 и 2 ОС «Astra Linux Special Edition».

Схема стенда представлена на рисунке ниже.

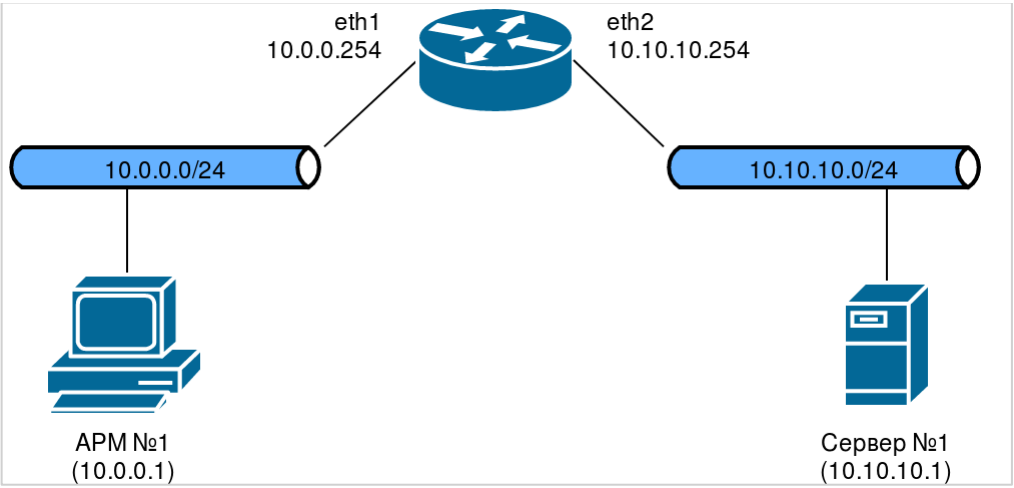


Рисунок 36 – Схема стенда

Рассматриваемый стенд состоит из:

- АРМ №1 (под управлением ОС «Astra Linux Special Edition») с ip-адресом 10.0.0.1/24.
- Сервер №1 (под управлением ОС «Astra Linux Special Edition») с ip-адресом 10.10.10.1/24.
- Изделие Numa Edge, являющееся шлюзом по умолчанию для АРМ№1 и Сервер №1, с адресами 10.0.0.254/24 (порт eth1, подключен к АРМ №1) и 10.10.10.254/24 (порт eth2, подключен к Сервер №1).

В информационной системе используется 4 уровня конфиденциальности (степени секретности) – от 0 до 3 включительно (в соответствии с ОС «Astra Linux Special Edition»). Процесс конфигурирования ОС «Astra Linux Special Edition» выходит за пределы данной инструкции и предполагается, что уже реализован должным образом.

Для создания политики межсетевого экранирования по классификационным меткам необходимо выполнить следующие действия в режиме настройки:

Пример 169 – Фильтрация по классификационным меткам

Действие	**Команда**
Создание именованных категорий для их дальнейшего использования в фильтрах трафика.	[edit] admin@Edge1# set system mac category c6 index '6' [edit] admin@Edge1# set system mac category c5 index '5'
Определение фильтра трафика sec-c – соответствующего уровню конфиденциальности 1.	[edit] admin@Edge1# set filter sec-c rule 10 mcs category 'c6' [edit] admin@Edge1# set filter sec-c rule 10 mls level 'unclassified'
Определение фильтра трафика sec-s – соответствующего уровню конфиденциальности 2.	[edit] admin@Edge1# set filter sec-s rule 10 mcs category 'c5' [edit] admin@Edge1# set filter sec-s rule 10 mls level 'unclassified'
Определение фильтра трафика sec-ts – соответствующего уровню конфиденциальности 3.	[edit] admin@Edge1# set filter sec-ts rule 10 mcs category 'c5' [edit] admin@Edge1# set filter sec-ts rule 10 mcs category 'c6' [edit] admin@Edge1# set filter sec-ts rule 10 mcs mode 'all' [edit] admin@Edge1# set filter sec-ts rule 10 mls level 'unclassified'
Создание политики фильтрации, разрешающей прохождение трафика соответствующего фильтрам sec-s и sec-c и запрещающей иные соединения.	[edit] admin@Edge1# set policy firewall fw rule 10 action 'drop' [edit] admin@Edge1# set policy firewall fw rule 10 match filter 'sec-ts' [edit] admin@Edge1# set policy firewall fw rule 20 action 'accept' [edit] admin@Edge1# set policy firewall fw rule 20 match filter 'sec-s' [edit] admin@Edge1# set policy firewall

Действие	Команда
	fw rule 30 action 'accept' [edit] admin@Edge1# set policy firewall fw rule 30 match filter 'sec-c' [edit] admin@Edge1# set policy firewall fw default-action 'drop'
Применение политики к входящим пакетам на интерфейсе eth0.	[edit] admin@Edge1# set interfaces ethernet eth1 policy in firewall 'fw'
Фиксация настройки.	[edit] admin@Edge1# commit

19.3 Команды настройки фильтрации по классификационным (мандатным) меткам.

Команды настройки	
system mac level <имя_уровня> label <значение_метки>	Настройка уровней мандатного доступа.
system mac category <имя_категории> index <индекс>	Настройка категорий мандатного доступа.
filter <имя> rule <номер_правила> mls level <уровень>	Указание уровня мандатного доступа для проверки соответствия в правиле фильтрации трафика.
filter <имя> rule <номер_правила> mls invert	Инверсия сопоставления для указанного уровня мандатного доступа.
filter <имя> rule <номер_правила> mcs category <категория>	Указание категорий мандатного доступа для проверки соответствия в правиле фильтрации трафика.
filter <имя> rule <номер_правила> mcs invert	Инверсия сопоставления для указанных категорий мандатного доступа
filter <имя> rule <номер_правила> mcs mode <режим>	Указание режима сопоставления категорий мандатного доступа.

19.3.1 system mac level <имя_уровня> label <значение_метки>

Настройка именованных уровней мандатного доступа для их дальнейшего использования в системе.

Синтаксис

```
set system mac level <имя_уровня> label <значение_метки>
delete system mac level <имя_уровня>
show system mac level <имя_уровня>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   mac {
      level имя_уровня {
         label значение_метки
      }
   }
}
```

Параметры

имя_уровня

Имя уровня мандатного контроля доступа.

значение_метки

Числовое значение метки уровня. Значение должно лежать в диапазоне от 0 до 255.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда предназначена для настройки доступных для использования в системе именованных уровней мандатного доступа.

По умолчанию в системе преднастроено 4 уровня определенных в RFC 1108:

- unclassified (неопределенно) — 10101011;
- confidential (конфиденциально) — 10010110;
- secret (секретно) — 01011010;
- top-secret (совершенно секретно) — 00111101.

Форма **set** данной команды используется для настройки уровней мандатного контроля доступа.

Форма **delete** данной команды используется для удаления настроенных уровней мандатного контроля доступа.

Форма **show** данной команды используется для отображения значений настроенных уровней мандатного контроля доступа.

19.3.2 system mac category <имя_категории> index <индекс>

Настройка именованных органов по защите (Protection Authority) для их дальнейшего использования в системе.

Синтаксис

```
set system mac <имя_категории> index <индекс>
delete system mac <имя_категории>
show system mac <имя_категории>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   mac {
      category имя_категории {
         index индекс
      }
   }
}
```

Параметры

имя_категории

Имя категории мандатного доступа.

индекс

Индекс бита в поле Protection Authority Flags. Значение должно лежать в диапазоне от 0 до 63.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда предназначена для настройки доступных для использования в системе органов по защите (Protection Authority) и назначения им соответствующих битов в поле Protection Authority Flags сетевого пакета.

По умолчанию в системе преднастроено 5 именованных органов по защите определенных в RFC 1108:

Последовательный номер бита	Наименование органа по защите
0	GENSER
1	SIOP-ESI
2	SCI
3	NSA
4	DOE

Форма **set** данной команды используется для настройки категории мандатного контроля доступа.

Форма **delete** данной команды используется для удаления категории мандатного контроля доступа.

Форма **show** данной команды используется для отображения значения индекса категории мандатного контроля доступа.

19.3.3 filter <имя> rule <номер_правила> mls level <уровень>

Указание уровня мандатного доступа для проверки соответствия в правиле фильтрации трафика.

Синтаксис

```
set filter <имя> rule <номер_правила> mls level <уровень>
delete filter <имя> rule <номер_правила> mls level
show filter <имя> rule <номер_правила> mls level
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      mls {
         level уровень
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

уровень

Уровень мандатного доступа. Данное правило будет применено к пакетам, уровень мандатного доступа которых соответствует указанному. Допустимые значения определяются командой system mac level.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для указания уровня мандатного доступа в правиле фильтрации трафика.

Форма **delete** данной команды используется для удаления уровня мандатного доступа в правиле фильтрации трафика.

Форма **show** данной команды используется для отображения текущей настройки.

19.3.4 filter <имя> rule <номер_правила> mls invert

Инверсия сопоставления уровня мандатного доступа для указанного правила фильтра.

Синтаксис

```
set filter <имя> rule <номер_правила> mls invert
delete filter <имя> rule <номер_правила> mls invet
show filter <имя> rule <номер_правила> mls
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      mls {
         invert
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет инверсировать сопоставление для выбранного мандатного уровня – при применении указанной команды в правиле фильтра, соответствующий фильтр будет определять сетевой трафик с мандатным уровнем отличным от заданного командой **filter <имя> rule <номер_правила> mls level <уровень>**.

Форма **set** данной команды используется для указания инверсирования мандатного уровня.

Форма **delete** данной команды позволяет восстановить поведение по умолчанию.

Форма **show** данной команды позволяет отобразить настройку.

19.3.5 filter <имя> rule <номер_правила> mcs category <категория>

Указание Protection Authority Flags для проверки соответствия в правиле фильтрации трафика.

Синтаксис

```
set filter <имя> rule <номер_правил>a mls category <категория>
delete filter <имя> rule <номер_правила> mls category <категория>
show filter <имя> rule <номер_правила> mls category
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      mcs {
         category категория
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

категория

Множественный параметр. Наименование органа по защите. Данное правило будет применено к пакетам, содержащим в поле Protection Authority Flags биты соответствующие заданным. Допустимые значения определяются командой **system mac category**.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для указания соответствия битов в поле Protection Authority Flags сетевых пакетов.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения заданных настроек.

19.3.6 filter <имя> rule <номер_правила> mcs invert

Инверсия сопоставления для поля Protection Authority Flags соответствующего правила фильтра.

Синтаксис

```
set filter <имя> rule <номер_правила> mcs invert
delete filter <имя> rule <номер_правила> mcs invert
show filter <имя> rule <номер_правила> mcs
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      mcs {
         invert
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет инверсировать сопоставление заданных Protection Authority Flags – при применении указанной команды в правиле фильтра, соответствующий фильтр будет определять сетевой трафик, не содержащий соответствующих битов в поле Protection Authority Flags сетевого пакета (заданных командой **filter <имя> rule <номер_правила> mcs category <категория>**).

Форма **set** данной команды используется для указания инверсирования сопоставления правила фильтра.

Форма **delete** данной команды позволяет восстановить поведение по умолчанию.

Форма **show** данной команды позволяет отобразить настройку.

19.3.7 filter <имя> rule <номер_правила> mcs mode <режим>

Указание режима сопоставления битов в поле Protection Authority Flags сетевого пакета.

Синтаксис

```
set filter <имя> rule <номер_правила> mcs mode <режим>
delete filter <имя> rule <номер_правила> mcs mode
show filter <имя> rule <номер_правила> mcs mode
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
filter имя {
   rule номер_правила {
      mcs {
         mode режим
      }
   }
}
```

Параметры

имя

Имя фильтра трафика.

номер_правила

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

режим

Указание режима проверки сопоставления. Допустимые значения:

all: Совпадение со всеми указанными битами;

any: Совпадение с любым из указанных битов Protection Authority Flags.

Значение по умолчанию

По умолдчанию используется значение any.

Указания по использованию

Данная команда позволяет установить режим проверки сопоставления установленных командой **filter <имя> rule <номер_правила> mcs category <категория>** битов в поле Protection Authority Flags сетевого пакета.

Форма **set** данной команды используется для указания режима проверки.

Форма **delete** данной команды позволяет восстановить режим проверки по умолчанию.

Форма **show** данной команды позволяет отобразить установленный режим проверки.

20 Политика межсетевого экранирования

20.1 Обзор межсетевого экрана

В данном разделе представлен обзор защитных функций межсетевого экрана Numa Edge.

Рассматриваются следующие вопросы:

- Функциональность межсетевого экрана Numa Edge
- Определение политик межсетевого экранирования
- Правила политик межсетевого экрана
- Правила исключения
- Межсетевой экран с поддержкой состояния и отслеживание подключений
- Применение политик межсетевого экранирования к интерфейсам
- Политики межсетевого экранирования IPv6
- Взаимодействие между межсетевыми экраном, NAT и маршрутизацией

20.1.1 Функциональность межсетевого экрана Numa Edge

Функциональность межсетевого экрана предназначена для анализа и фильтрации пакетов IP между сетевыми интерфейсами. Ее наиболее частое применение – защита трафика между внутренней сетью и Интернетом. Она позволяет фильтровать пакеты на основе их характеристик и выполнять действия над пакетами, соответствующими правилу. Функциональность межсетевого экрана Numa Edge предоставляет следующие возможности:

- Фильтрация пакетов для транзитного (forwarded) трафика, проходящего через маршрутизатор, при помощи ключевых слов **in** и **out** на интерфейсе.
- Фильтрация пакетов для трафика, предназначенного самому маршрутизатору, при помощи ключевого слова **local.**
- Выборка трафика для правил при помощи фильтров.
- Перенаправление сетевого трафика IPv4/IPv6, соответствующего заданным критериям правила, на указанный шлюз.

В межсетевом экране Numa Edge представлена проверка пакетов с поддержкой состояния, так что он может обеспечить существенную дополнительную защиту в многоуровневой стратегии безопасности. Система может перехватывать активность в сети, относить ее к категориям в соответствии с настроенной в ней базой данных разрешенного трафика и разрешать или отвергать попытку.

20.1.2 Определение политик межсетевого экранирования

Чтобы использовать функцию межсетевого экрана, следует определить набор правил ("политику") межсетевого экранирования и сохранить его с некоторым именем. Политика межсетевого экранирования состоит из ряда правил. После создания политика применяется к интерфейсу для фильтрации пакетов.

20.1.3 Правила политик межсетевого экрана

Правила политик межсетевого экранирования используют фильтры, в которых указываются условия соответствия для трафика. Правило определяет действия, которые должны быть предприняты, если условия соответствия, прописанные в фильтрах, выполняются. Соответствие трафика может проверяться фильтрами по ряду характеристик, в том числе по IP-адресу отправителя, IP-адресу получателя, порту отправителя, порту получателя, протоколу IP и типу ICMP. Для настройки правил сетевого трафика IPv4 используется ветвь конфигурации **policy firewall**. Для настройки правил сетевого трафика IPv6 используется ветвь конфигурации **policy firewall-ipv6**.

Правила выполняются последовательно в соответствии с номером правила. Если трафик соответствует характеристикам, указанным в правиле, то выполняется действие правила; если не соответствует, то система переходит к следующему правилу.

Действие может быть одним из следующих:

- **Принять (accept).** Трафик разрешается и пересылается.
- **Игнорировать (drop)**. Трафик отбрасывается без каких бы то ни было действий.

- **Отвергнуть (reject)**. Трафик отбрасывается со сбросом TCP.
- **Проверить (inspect)**. Трафик обрабатывается системой защиты от вторжений (IPS).
- **Задержать (tarpit).** Подвесить входящее TCP соединение
- **Обмануть (delude).** Создать видимость открытого TCP порта.

По умолчанию в любой политике межсетевого экранирования есть неявное окончательное действие **drop** (сброс). Это значит, что трафик, не соответствующий ни одному правилу политики, отбрасывается без каких бы то ни было действий. Действие по умолчанию может быть изменено при помощи команды **policy firewall** <имя> **default-action** <действие> для протокола IPv4, либо **policy firewall-ipv6** <имя> **default-action** <действие> для протокола IPv6, соответственно.

20.1.4 Правила исключения

Следует обратить внимание, что нужно проявлять аккуратность при использовании более чем одного правила «исключения» (то есть правила, в котором используется операция отрицания ("!") для исключения правила из обработки). Проверка соответствия правилам выполняется последовательно, так что последовательность из правил исключения может привести к поведению, отличному от ожидаемого.

20.1.5 Межсетевой экран с поддержкой состояния и отслеживание подключений

Интерфейс командной строки Numa Edge взаимодействует с системой отслеживания подключений сетевого фильтра, которая является модулем, обеспечивающим отслеживание подключений для различных функций системы, в том числе для межсетевого экрана, NAT и балансировки нагрузки ГВС. В межсетевом экране отслеживание подключений делает возможной проверку пакетов с поддержкой состояния.

В отличие от межсетевых экранов без поддержки состояния, фильтрующих пакеты по отдельности на основе статических сведений об отправителе и получателе, межсетевые экраны с поддержкой состояния отслеживают состояние сетевых подключений и потоки трафика и разрешают или ограничивают трафик на основе состояния известности и желательности его подключения. Хотя межсетевые экраны с поддержкой состояния при высокой нагрузке работают медленнее межсетевых экранов без поддержки состояния, первые лучше блокируют нежелательную связь.

Параметры поддержки состояния по умолчанию могут быть изменены командами **system conntrack table-size** <размер> и **system conntrack tcp-loose** <состояние>.

20.1.6 Применение политик межсетевого экранирования к интерфейсам

Когда политика межсетевого экранирования определена, её можно применить к интерфейсам, и она будет работать как пакетный фильтр. Политика межсетевого экранирования фильтрует пакеты одним из следующих способов в зависимости от того, что указано при её применении:

- **in** (входящий). Если применить политику с использованием ключевого слова **in**, межсетевой экран будет фильтровать транзитный сетевой трафик, входящий в интерфейс и проходящий через Numa Edge. (Сюда не относится сетевой трафик предназначенный для самого МЭ) С использованием ключевого слова **in** можно применить один пакетный фильтр.
- **out** (исходящий). Если применить политику с использованием ключевого слова **out,** межсетевой экран будет фильтровать транзитный сетевой трафик, покидающий интерфейс. (Сюда не относятся пакеты, исходящие от самого МЭ). С использованием ключевого слова **out** можно применить один пакетный фильтр.
- **local** (локальный). Если применить политику с использованием ключевого слова **local**, межсетевой экран будет фильтровать пакеты, предназначенные для Numa Edge, входящие на интерфейсе. С использованием ключевого слова **local** можно применить один пакетный фильтр.

К интерфейсу может быть применено не более трёх политик межсетевого экранирования: одна с указанием ключевого слова **in**, одна – с указанием ключевого слова **out** и одна – с указанием ключевого слова **local**.

20.1.7 Политики межсетевого экранирования IPv6

Защита, обеспечиваемая межсетевым экраном, для сайтов, использующих IPv6, очень важна, так как протокол IPv6 не предоставляет функциональности NAT. Таким образом, межсетевой экран является единственным способом защиты сети IPv6.

Следует заметить, что политики межсетевого экранирования задаются для IPv4 и для IPv6 независимо. Пакеты IPv4 не проверяются по правилам в политиках IPv6, и наоборот. Пакеты IPv6 проверяются ТОЛЬКО по

правилам в таблице фильтра для IPv6, а пакеты IPv4 проверяются ТОЛЬКО по правилам в таблице фильтра для протокола IPv4.

В общем, поддержка IPv6 для межсетевого экрана параллельна поддержке для межсетевого экрана IPv4. Некоторые параметры, характерные для IPv4, не применяются в политиках межсетевого экранирования IPv6 и наоборот, например:

- У протокола ICMP есть версия, характерная для IPv6: "ICMP для IPv6". Потому в межсетевом экране IPv6 имеется дополнительное ключевое слово **icmpv6** для параметра фильтрации **protocol**. По той же причине ключевое слово **icmp** для межсетевого экрана IPv6 не поддерживается.
- Параметр **fragment** не поддерживается для межсетевого экрана IPv6, так как фрагментация к IPv6 неприменима.

В IPv4 сопоставление L2-адреса (MAC-адреса сетевого адаптера) с L3-адресом (IP-адресом) в рамках широковещательного домена осуществляется посредством протокола ARP. ARP является протоколом канального уровня и не будет обработан политикой firewall или firewall-ipv6. В IPv6 сопоставление L2-адреса (MAC-адреса сетевого адаптера) с L3-адресом (IP-адресом) в рамках широковещательного домена осуществляется посредством части протоколов из NDP (Neighbor Discovery Protocol). Протоколы NDP используют IPV6. В связи с этим, протоколы, входящие в NDP, будут обработаны политикой firewall-ipv6.

В связи с этим, установка политики policy firewall для направления трафика local никак не повлияет на транзитный трафик IPv4, в то время как установка политики firewall-ipv6 для направления трафика local может полностью блокировать как транзитный трафик, так и локальный IPv6 трафик в связи с тем, что политикой могут быть блокированы запросы на сопоставления L2-адреса (MAC-адреса сетевого адаптера) с L3-адресом (IP-адресом).

Для того, чтобы была возможность сопоставления L2-адреса (MAC-адреса сетевого адаптера) с L3-адресом (IP-адресом) для IPv6 необходимо в политику policy firewall-ipv6 добавить фильтр, первые два правила которого должны выглядеть следующим образом:

```
[edit]
admin@edge# set filter-ipv6 HOP-LIMIT-FILTER rule 10 icmpv6 type neighbour-
solicitation
[edit]
admin@edge# set filter-ipv6 HOP-LIMIT-FILTER rule 10 protocol icmpv6
[edit]
admin@edge# set filter-ipv6 HOP-LIMIT-FILTER rule 20 icmpv6 type neighbour-
advertisement
[edit]
admin@edge# set filter-ipv6 HOP-LIMIT-FILTER rule 20 protocol icmpv6
```

20.1.8 Взаимодействие между межсетевыми экраном, NAT и маршрутизацией

Один из наиболее важных моментов, с которыми следует ознакомиться при работе с межсетевым экраном, это порядок обработки различных служб, которые могут быть настроены в Numa Edge. Если порядок обработки не принимается во внимание, полученные результаты могут отличаться от ожидаемых. На рисунке ниже показан поток трафика через межсетевой экран, NAT и службы маршрутизации внутри Numa Edge.

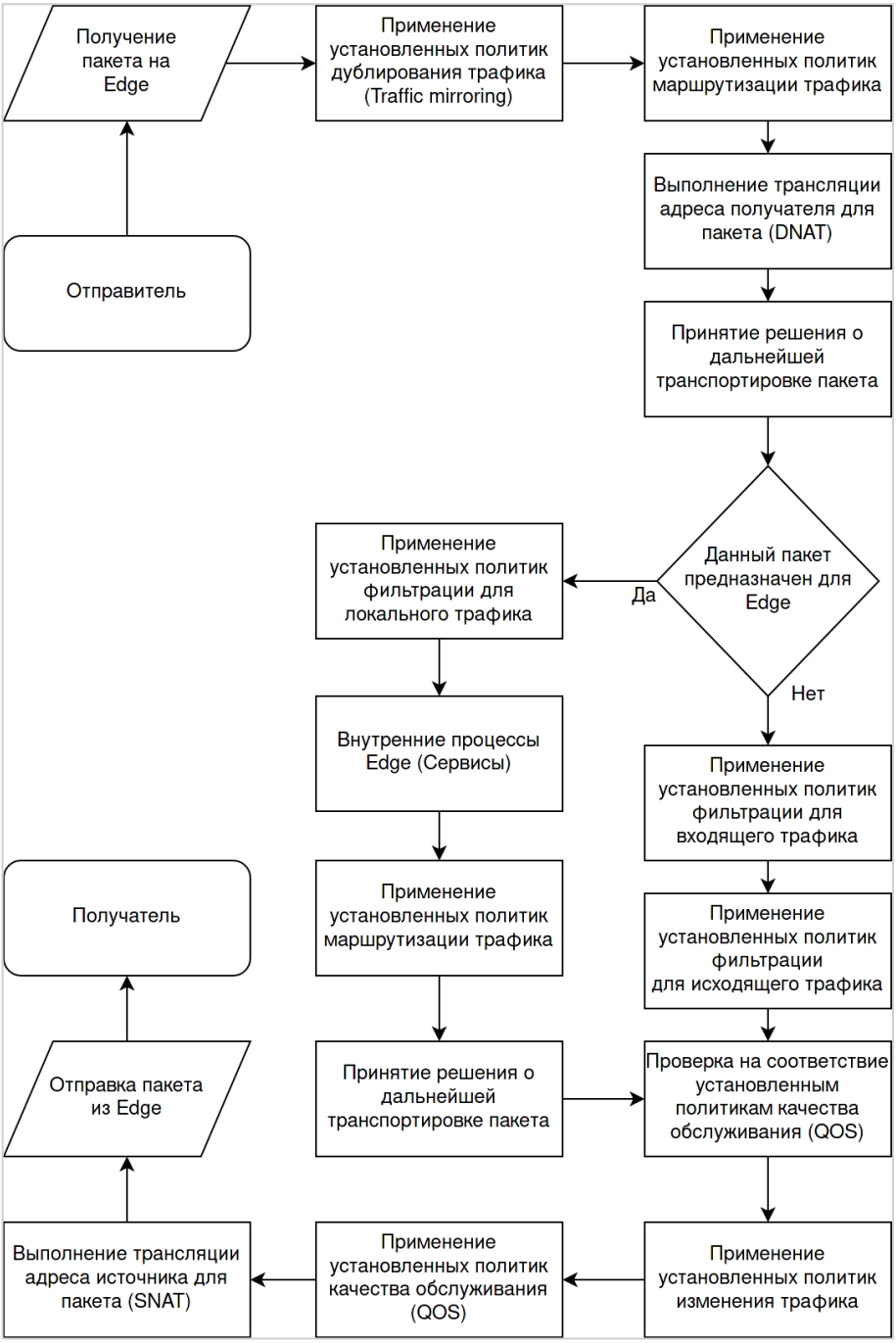


Рисунок 37 – Прохождение трафика через Numa Edge

Под блоком "Применение установленных политик маршрутизации трафика" подразумевается Policy-Based-Routing (PBR).

На рисунке ниже изображена базовая схема сети, которая будет использоваться в дальнейших примерах фильтрации трафика.

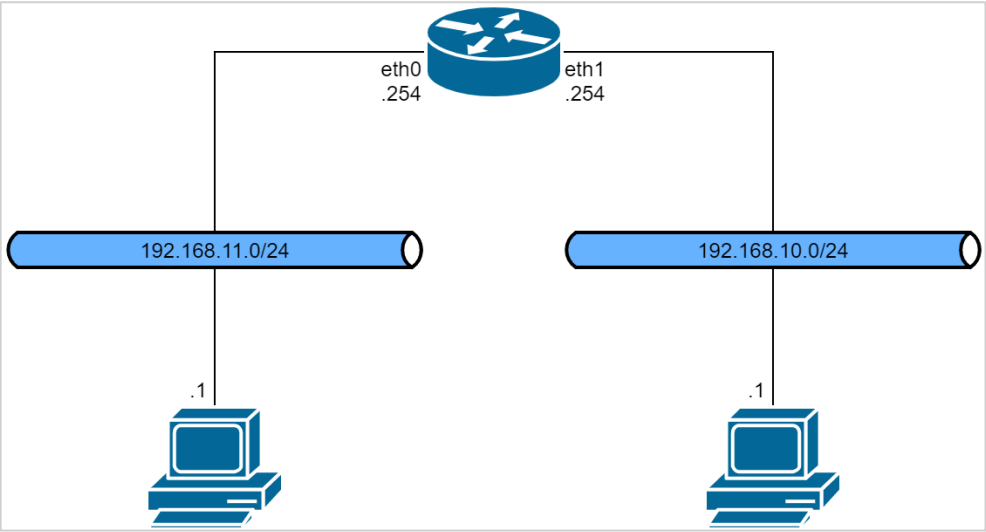


Рисунок 38- Базовая схема

Пример 1: прохождение транзитного трафика через Numa Edge; фильтрация транзитного трафика, приходящего на интерфейс

На рисунке ниже оказаны взаимосвязи между межсетевым экраном, NAT и маршрутизацией в Numa Edge по ходу потока транзитного трафика (проходящего сквозь систему) и политики межсетевого экранирования, применённые к трафику, принимаемому (**in**) на интерфейсе.

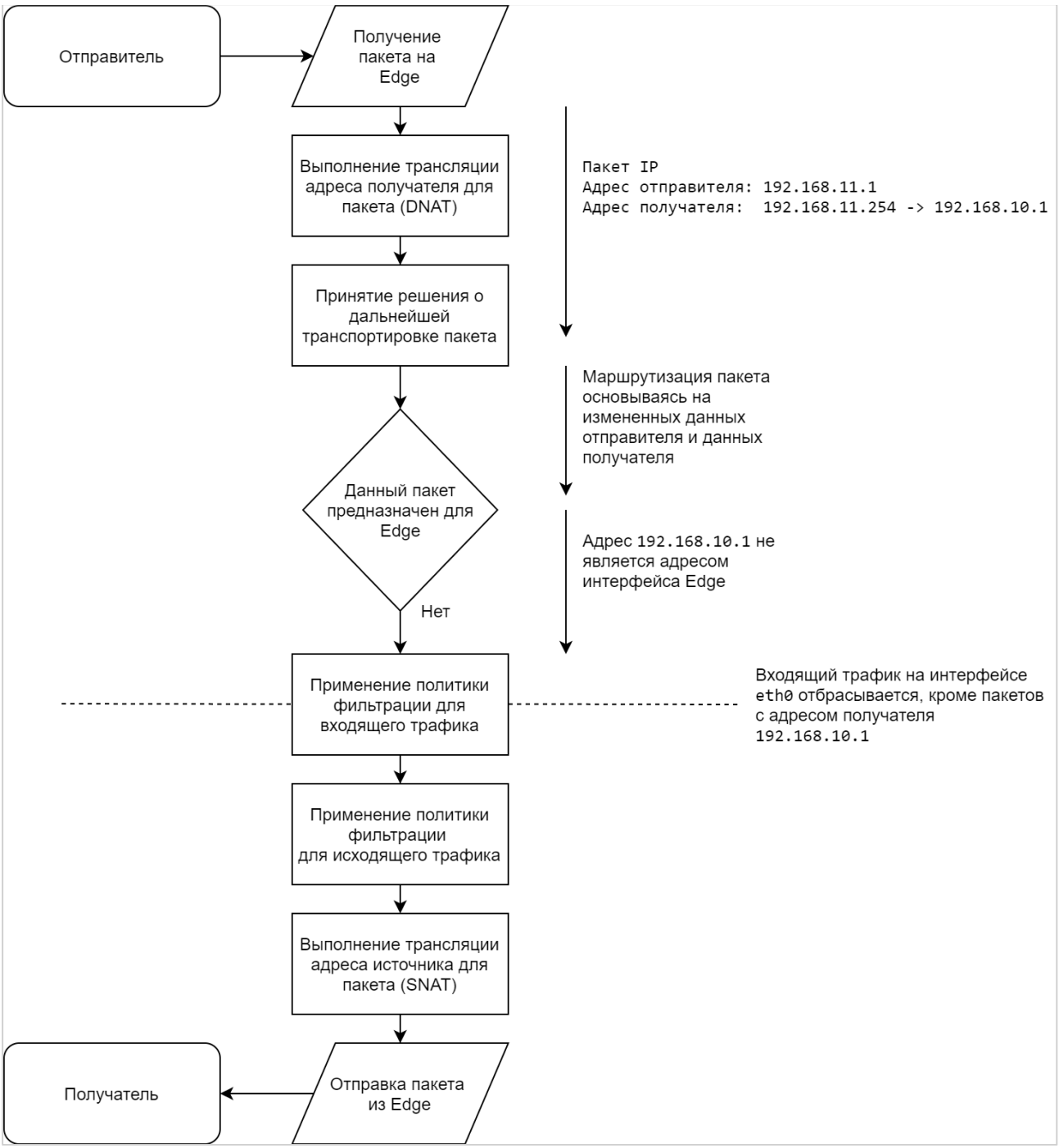


Рисунок 39 – Применение правил фильтрации к транзитному трафику, получаемому на интерфейсе

Настройка, выполненная на Numa Edge (не включает в себя описание DNAT и SNAT):

Действие	**Команда**
Определение фильтра трафика FW-dst.	`[edit]` `admin@edge# set filter FW-dst`
Фильтр FW-dst определяет трафик, получателем которого является 192.168.10.1.	`[edit]` `admin@edge# set filter FW-dst rule 10 destination address 192.168.10.1`
Фильтр FW-det определяет трафик, относящийся к протоколу TCP.	`[edit]` `admin@edge# set filter FW-dst rule 10 protocol tcp`
Создание узла конфигурации для политики межсетевого экранирования FW-in, для которой по умолчанию определен	`[edit]` `admin@edge# set policy firewall FW-in default-action drop`

Действие	Команда
запрет на прохождение трафика.	
Создание правила Rule 10 для политики межсетевого экранирования FW-in. Это правило разрешает прохождение трафика, соответствующего только указанным критериям.	`[edit]` `admin@edge# set policy firewall FW-in rule 10 action accept`
В качестве критериев для правила Rule 10 определено соответствие трафика фильтру FW-dst.	`[edit]` `admin@edge# set policy firewall FW-in rule 10 match filter FW-dst`
Применение политики межсетевого экранирования FW-in к транзитному входящему трафику интерфейса eth0.	`[edit]` `admin@edge# set interfaces ethernet eth0 policy in firewall FW-in`
Фиксация настройки.	`[edit]` `admin@edge# commit`

Просмотр внесенных изменений.	`[edit]`
	`admin@edge# show filter FW-dst`
	`{`
	`rule 10 {`
	`destination {`
	`address 192.168.10.1`
	`}`
	`protocol tcp`
	`}`
	`}`
	`interfaces {`
	`ethernet eth0 {`
	`address 192.168.11.254/24`
	`duplex auto`
	`mtu 1500`
	`policy {`
	`in {`
	`firewall FW-in`
	`}`
	`}`
	`speed auto`
	`} }... policy {`
	`firewall FW-in {`
	`default-action drop`
	`rule 10 {`
	`action accept`
	`match {`
	`filter FW-dst`
	`}`
	`}`
	`}`
	`}`

Соответствие политикам межсетевого экранирования проверяется после DNAT и решений о маршрутизации, но до SNAT. Именно по этому в качестве адреса получателя указывается адрес, фигурирующий в пакетах после выполнения DNAT.

Пример 2: прохождение транзитного трафика через Numa Edge; фильтрация транзитного трафика, уходящего через интерфейс

На рисунке ниже показаны взаимосвязи между межсетевым экраном, NAT и маршрутизацией в Numa Edge по ходу потока транзитного трафика (проходящего сквозь систему) и экземпляры межсетевого экрана, применённые к трафику, уходящему (**out**) через интерфейс.

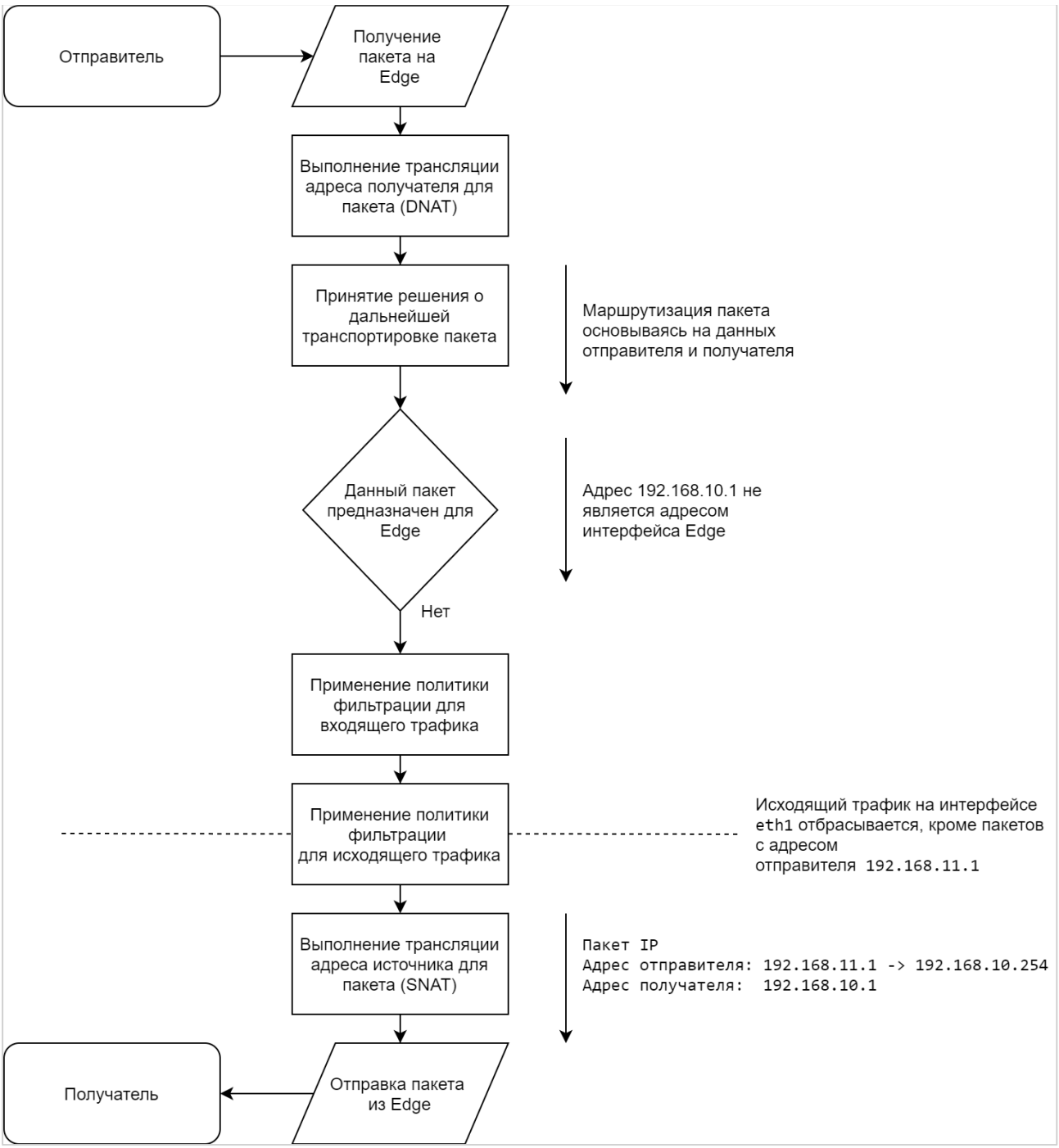


Рисунок 40 – Применение правил фильтрации к транзитному трафику, отправляемому через интерфейс

Настройка, выполненная на Numa Edge (не включает в себя описание DNAT и SNAT):

Действие	**Команда**
Определение фильтра трафика FW-src.	`[edit]` `admin@edge# set filter FW-src`
Фильтр FW-src определяет трафик, источником которого является 192.168.11.1.	`[edit]` `admin@edge# set filter FW-src rule 10 source address 192.168.11.1`
Фильтр FW-src определяет трафик, относящийся к протоколу TCP.	`[edit]` `admin@edge# set filter FW-src rule 10 protocol tcp`
Создание узла конфигурации для политики межсетевого экранирования FW-out, для которой по умолчанию определен	`[edit]` `admin@edge# set policy firewall FW-out default-action drop`

Действие	Команда
запрет на прохождение трафика.	
Создание правила Rule 10 для политики межсетевого экранирования FW-out. Это правило разрешает прохождение трафика, соответствующего только указанным критериям.	`[edit]` `admin@edge# set policy firewall FW-out rule 10 action accept`
В качестве критериев для правила Rule 10 определено соответствие трафика фильтру FW-src.	`[edit]` `admin@edge# set policy firewall FW-out rule 10 match filter FW-src`
Применение политики межсетевого экранирования FW-out к исходящему транзитному трафику интерфейса eth1.	`[edit]` `admin@edge# set interfaces ethernet eth1 policy out firewall FW-out`
Фиксация настройки.	`[edit]` `admin@edge# commit`

Просмотр внесенных изменений.	`[edit]`
	`admin@edge# show filter FW-src`
	`{`
	`rule 10 {`
	`source {`
	`address 192.168.11.1`
	`}`
	`protocol tcp`
	`}`
	`}`
	`interfaces {`
	`ethernet eth1 {`
	`address 192.168.10.254/24`
	`duplex auto`
	`mtu 1500`
	`policy {`
	`out {`
	`firewall FW-out`
	`}`
	`}`
	`speed auto`
	`} }... policy {`
	`firewall FW-out {`
	`default-action drop`
	`rule 10 {`
	`action accept`
	`match {`
	`filter FW-src`
	`}`
	`}`
	`}`
	`}`

Следует заметить, что соответствие политикам межсетевого экранирования проверяется после DNAT и решений о маршрутизации, но до SNAT. Именно по этому в качестве адреса отправителя указывается адрес, фигурирующий в пакетах до выполнения SNAT.

Пример 3: прохождение трафика, направленного в локальную систему, через Numa Edge; его фильтрация при вхождении на интерфейс

На рисунке ниже показаны взаимосвязи между межсетевым экраном, NAT и маршрутизацией в Numa Edge по ходу потока трафика, приходящего в сам Numa Edge и политики межсетевого экранирования, применённые к локальному **(local)** трафику на интерфейсе.

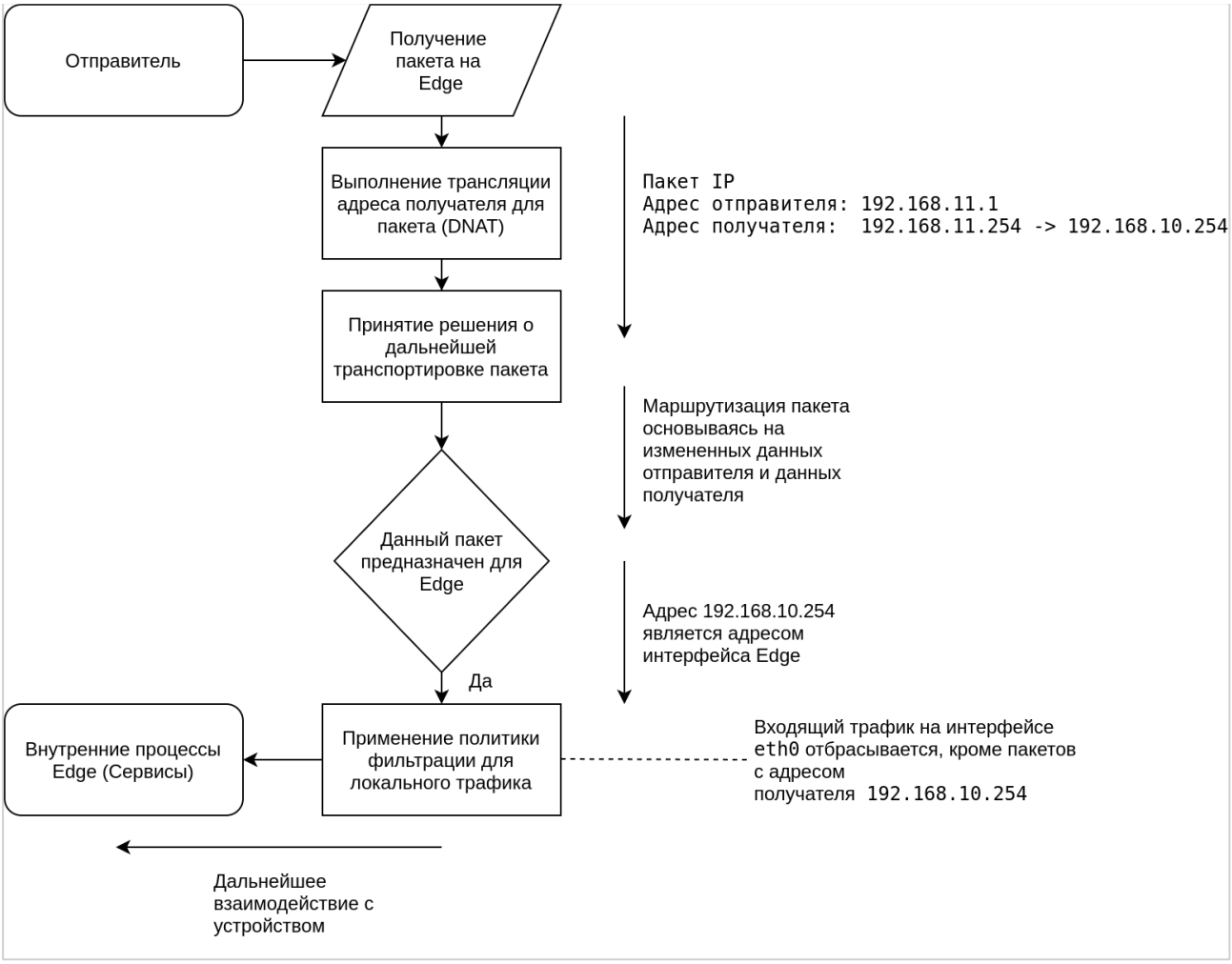


Рисунок 41 – Применение правил фильтрации к трафику, предназначенному локальной системе, получаемому на интерфейсе

Настройка, выполненная на Numa Edge (не включает в себя описание DNAT и SNAT):

Действие	**Команда**
Определение фильтра трафика FW-dst-2.	`[edit]` `admin@edge# set filter FW-dst-2`
Фильтр FW-dst-2 определяет трафик, получателем которого является 192.168.10.1.	`[edit]` `admin@edge# set filter FW-dst-2 rule 10 destination address 192.168.10.254`
Фильтр FW-dst-2 определяет трафик, относящийся к протоколу TCP.	`[edit]` `admin@edge# set filter FW-dst-2 rule 10 protocol tcp`
Создание узла конфигурации для политики межсетевого экранирования FW-local, для которой по умолчанию определен запрет на прохождение трафика.	`[edit]` `admin@edge# set policy firewall FW-local default-action drop`
Создание правила Rule 10 для политики межсетевого экранирования FW-local. Это правило разрешает прохождение трафика, соответствующего только указанным критериям.	`[edit]` `admin@edge# set policy firewall FW-local rule 10 action accept`
В качестве критериев для правила Rule 10 определено соответствие трафика фильтру FW-dst-2.	`[edit]` `admin@edge# set policy firewall FW-local rule 10 match filter FW-dst-2`
Применение политики межсетевого экранирования FW-local к входящему трафику интерфейса eth0, предназначенному для Edge.	`[edit]` `admin@edge# set interfaces ethernet eth0 policy local`

Действие	Команда
	`firewall FW-local`
Фиксация настройки.	`[edit]` `admin@edge# commit`

Просмотр внесенных изменений.	`[edit]`
	`admin@edge# show filter FW-dst-2 {`
	`rule 10 {`
	`destination {`
	`address 192.168.10.254`
	`}`
	`protocol tcp`
	`}`
	`}`
	`interfaces {`
	`ethernet eth0 {`
	`address 192.168.11.254/24`
	`duplex auto`
	`mtu 1500`
	`policy {`
	`local {`
	`firewall FW-local`
	`}`
	`}`
	`speed auto`
	`} }... policy {`
	`firewall FW-local {`
	`default-action drop`
	`rule 10 {`
	`action accept`
	`match {`
	`filter FW-dst-2`
	`}`
	`}`
	`}`
	`}`

Следует заметить, что соответствие политикам межсетевого экранирования проверяется после DNAT и маршрутизации. В текущем варианте SNAT не выполняется.

Пример 4: прохождение трафика, направленного из локальной системы, через Numa Edge

На рисунке ниже показаны взаимосвязи между межсетевым экраном, NAT и маршрутизацией в Numa Edge по ходу потока трафика, исходящего из самого Numa Edge.

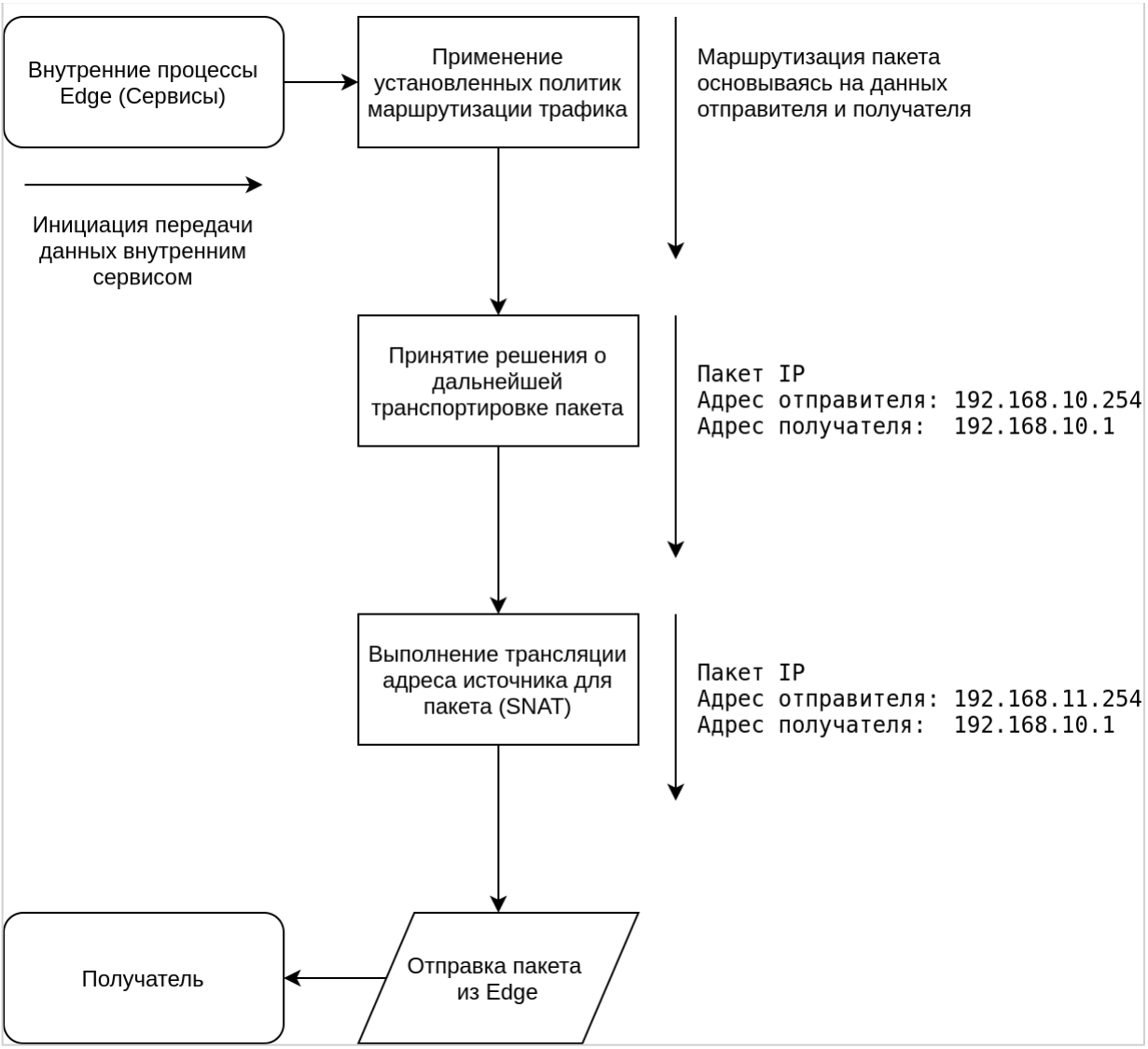


Рисунок 42 – Прохождение трафика, направленного из локальной системы

Следует отметить, что к сетевому трафику, исходящему из Numa Edge нельзя применить политики межсетевого экранирования. В текущем варианте DNAT не выполняется. Выполняется SNAT для исходящего трафика.

20.2 Примеры настройки

В этом разделе рассматриваются следующие вопросы:

- Фильтрация по IP-адресу отправителя.
- Фильтрация по IP-адресам отправителя и получателя.
- Фильтрация по IP-адресу отправителя и порту получателя.
- Фильтрация по подсетям отправителя и получателя.
- Фильтрация по MAC-адресу отправителя.
- Исключение адреса.
- Активация в течение указанных периодов времени.
- Ограничение скоростей передачи трафика.
- Проверка соответствия флагов TCP.
- Проверка соответствия имен типов ICMP.
- Проверка соответствия групп.
- Проверка соответствия недавно встречавшихся отправителей.

В этом разделе есть следующие примеры:

- Пример 170– Фильтрация по IP-адресу отправителя
- Пример 171– Фильтрация по IP-адресам отправителя и получателя
- Пример 172– Фильтрация по IP-адресу отправителя и протоколу получателя
- Пример 173– Фильтрация по подсетям отправителя и получателя
- Пример 174– Фильтрация по MAC-адресу отправителя
- Пример 175– Исключение адреса
- Пример 176– Активация в течение указанных периодов времени
- Пример 177– Принятие пакетов ICMP с конкретными именами типов
- Пример 178 – Ограничение скорости для конкретных входящих пакетов
- Пример 179– Принятие пакетов с установленными конкретными флагами TCP
- Пример 180– Отклонение трафика на основе групп адресов, сетей или портов
- Пример 181 – Игнорирование попыток подключения от одного и того же отправителя при превышении указанного порога их числа за данный промежуток времени

Примеры 170- 174 Соответствуют настройке межсетевого экрана 'Edge1', как показано на рисунке ниже.

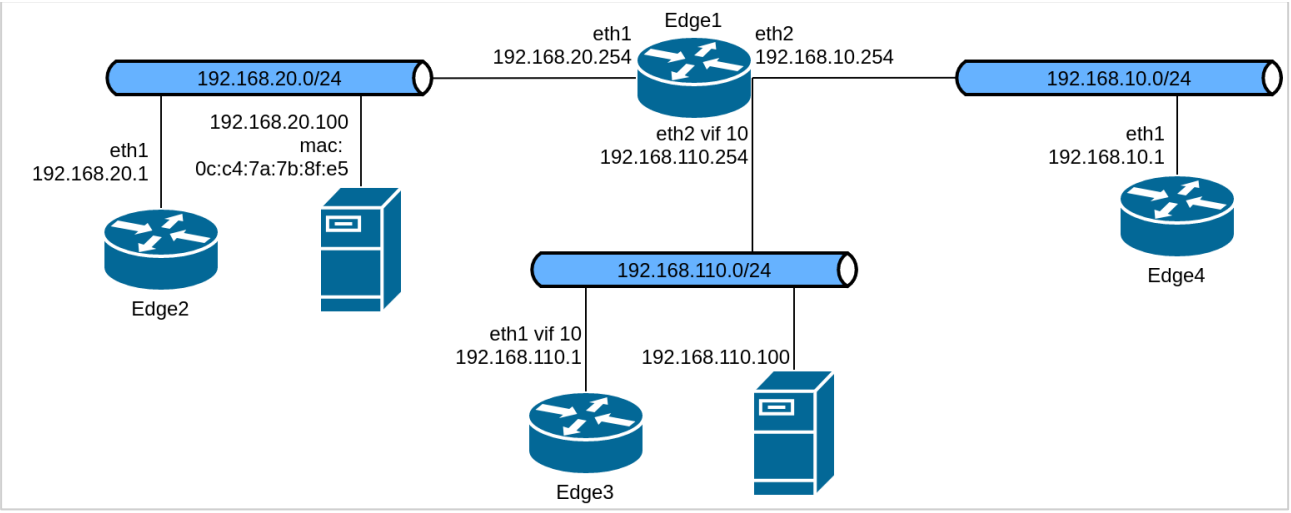


Рисунок 43 – Настройка межсетевого экрана для примеров 170- 174

Примеры 175-178 Соответствуют настройке межсетевого экрана 'edge', как показано на рисунке ниже.

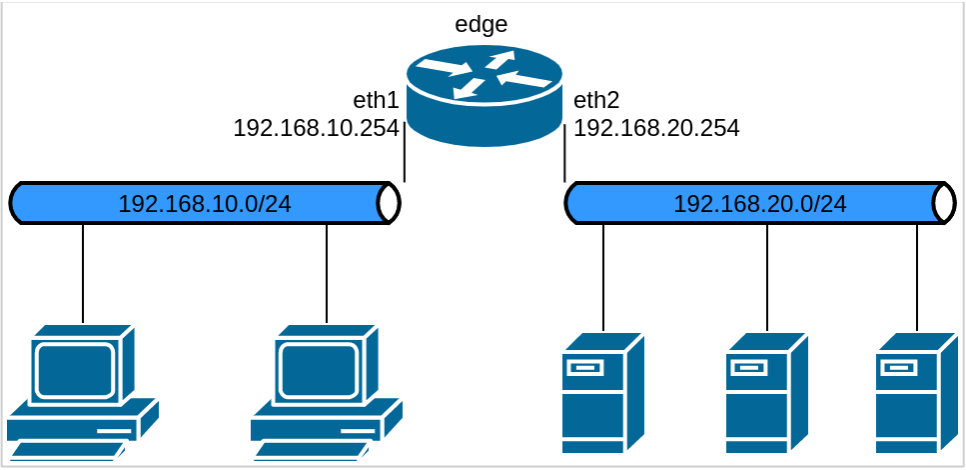


Рисунок 44 – Настройка межсетевого экрана для примеров 175-178

20.2.1 Фильтрация по IP-адресу отправителя

В примере ниже выполняется определение политики межсетевого экранирования, состоящей из одного правила для фильтрации только по IP-адресу отправителя. Это правило будет отклонять пакеты, приходящие с маршрутизатора 'Edge2'. Затем политика межсетевого экранирования применяется ко входящим пакетам на интерфейсе **eth1**.

Для создания политики для фильтрации по IP-адресу отправителя выполните следующие действия в режиме настройки:

Пример 170– Фильтрация по IP-адресу отправителя

Действие	**Команда**
Определение фильтра трафика, отправителем которого является 192.168.20.1.	`[edit]` `admin@Edge1# set filter FWTEST-1 rule 10 source address 192.168.20.1`
Определение политики межсетевого экранирования FW1.	`[edit]` `admin@Edge1# set policy firewall FW1`

Создание узла конфигурации для межсетевого экрана FW1 и его правила rule 10. Это правило отклоняет трафик, соответствующий фильтру FWTEST-1.	`[edit]`
	`admin@Edge1# set policy firewall FW1 rule 10 action drop`
	`[edit]`
	`admin@Edge1# set policy firewall FW1 rule 10 match filter FWTEST-1`

Установка для межсетевого экрана FW1 действия по умолчанию. Пакеты будут приниматься и пересылаться по умолчанию.	`[edit]` `admin@Edge1# set policy firewall FW1 default-action accept`
Применение FW1 ко входящим пакетам на интерфейсе eth1.	`[edit]` `admin@Edge1# set interfaces ethernet eth1 policy in firewall FW1`
Фиксация настройки.	`[edit]` `admin@Edge1# commit`

20.2.2 Фильтрация по IP-адресам отправителя и получателя

В примере ниже определяется ещё одна политика межсетевого экранирования. Она состоит из одного правила для фильтрации на основе IP-адресов как отправителя, так и получателя. Это правило принимает пакеты, исходящие из маршрутизатора 'Edge4' через интерфейс **eth1** с адресом 192.168.10.1 и предназначенные адресу 192.168.110.100. Затем политика применяется к пакетам, исходящим из виртуального интерфейса **vif 10** на интерфейсе **eth2**.

Для создания политики для фильтрации по IP-адресу отправителя и получателя выполните следующие действия в режиме настройки:

Пример 171– Фильтрация по IP-адресам отправителя и получателя

Действие	**Команда**
Определения фильтра трафика, отправителем которого является 192.168.10.1.	`[edit]` `admin@Edge1# set filter FWTEST-2 rule 10 source address 192.168.10.1`
Уточнение фильтра трафика – определение получателя сетевого трафика - 192.168.110.100.	`[edit]` `admin@Edge1# set filter FWTEST-2 rule 10 destination address 192.168.110.100`
Применение фильтра FWTEST-2 к политике межсетевого экрана FW2.	`[edit]` `admin@Edge1# set policy firewall FW2 rule 10 match filter FWTEST-2`
Создание узла конфигурации для межсетевого экрана FW2 и его правила rule 10. Это правило разрешает прохождение трафика, соответствующего фильтру FWTEST-2.	`[edit]` `admin@Edge1# set policy firewall FW2 rule 10 action accept`
Применение FW2 к исходящим пакетам на интерфейсе eth2 vif 10.	`[edit]` `admin@Edge1# set interfaces ethernet eth2 vif 10 policy out firewall FW2`
Фиксация настройки.	`[edit]` `admin@Edge1# commit`

20.2.3 Фильтрация по IP-адресу отправителя и порту получателя

В примере ниже определяется правило межсетевого экрана для фильтрации по IP-адресу отправителя и порту получателя. Это правило разрешает пакеты TCP, исходящие с адреса 192.168.10.1 (маршрутизатор 'Edge4') и предназначенные для порта telnet на 'Edge1'. Политика применяется к локальным пакетам (то есть пакетам, предназначенным для данного маршрутизатора 'Edge1'), приходящим через eth2.

Для создания политики для фильтрации по IP-адресу отправителя и протоколу получателя выполните следующие действия в режиме настройки:

Пример 172– Фильтрация по IP-адресу отправителя и протоколу получателя

Действие	**Команда**
Определение фильтра трафика FWTEST-3.	`[edit]` `admin@Edge1# set filter FWTEST-3`
Фильтр FWTEST-3 определяет трафик, отправителем которого является 192.168.10.1.	`[edit]` `admin@Edge1# set filter FWTEST-3 rule 10 source address 192.168.10.1`
Фильтр FWTEST-3 определяет трафик, относящийся к протоколу TCP.	`[edit]` `admin@Edge1# set filter FWTEST-3 rule 10 protocol tcp`
Фильтр FWTEST-3 определяет трафик, предназначенный для службы Telnet.	`[edit]` `admin@Edge1# set filter FWTEST-3 rule 10 destination port telnet`
Создание узла конфигурации для политики межсетевого экранирования FW3 и его правила rule 10. Это правило разрешает прохождение трафика, соответствующего только указанным критериям.	`[edit]` `admin@Edge1# set policy firewall FW3 rule 10 action accept`
Применение фильтра FWTEST-3 к политике межсетевого экрана FW3.	`[edit]` `admin@Edge1# set policy firewall FW3 rule 10 match filter FWTEST-3`
Применение FW3 к пакетам, предназначенным для данного маршрутизатора и приходящим на eth2.	`[edit]` `admin@Edge1# set interfaces ethernet eth2 policy local firewall FW3`
Фиксация настройки.	`[edit]` `admin@Edge1# commit`

20.2.4 Фильтрация по подсетям отправителя и получателя

В примере выполняется создание межсетевого пакетного фильтра, разрешающего пакеты, исходящие из 192.168.110/24 и предназначенные для 192.168.20.0/24. Затем экземпляр межсетевого фильтра применяется ко входящим пакетам с виртуального интерфейса vif 10 на интерфейсе eth2.

Для создания межсетевого фильтра выполните следующие действия в режиме настройки:

Пример 173– Фильтрация по подсетям отправителя и получателя

Действие	**Команда**
Создание фильтра сетевого трафика FWTEST-4.	`[edit]` `admin@Edge1# set filter FWTEST-4`
Фильтр FWTEST-4 определяет трафик, приходящий из сети 192.168.110.0/24.	`[edit]` `admin@Edge1# set filter FWTEST-4 rule 10 source address 192.168.110.0/24`
Фильтр FWTEST-4 определяет трафик, предназначенный для сети 192.168.20.0/24.	`[edit]` `admin@Edge1# set filter FWTEST-4 rule 10 destination address 192.168.20.0/24`
Создание узла конфигурации политики межсетевого экранирования FW4 и его правила rule 10. Это правило разрешает трафик, соответствующий указанным критериям.	`[edit]` `admin@Edge1# set policy firewall FW4 rule 10 action accept`
Применение фильтра FWTEST-4 к политике межсетевого экрана FW4.	`[edit]` `admin@Edge1# set policy firewall FW4 rule`

Действие	Команда
	10 match filter FWTEST-4
Применение политики межсетевого экранирования FW4 к пакетам, предназначенным для данного маршрутизатора и приходящим через виртуальный интерфейс vif 10 на eth2.	[edit] admin@Edge1# set interfaces ethernet eth2 vif 10 policy in firewall FW4
Фиксация настройки.	[edit] admin@Edge1# commit

20.2.5 Фильтрация по MAC-адресу отправителя

В примере ниже выполняется определение политики межсетевого экранирования, состоящей из одного правила для фильтрации только по MAC-адресу отправителя. Это правило будет разрешать пакеты, приходящие с конкретного компьютера, определяемого по его MAC-адресу, а не по IP-адресу. Политика межсетевого экранирования применяется ко входящим пакетам на интерфейсе **eth1**.

Для создания политики для фильтрации по MAC-адресу отправителя выполните следующие действия в режиме настройки:

Пример 174– Фильтрация по MAC-адресу отправителя

Действие	Команда
Задание параметров фильтра трафика FWTEST-5 – фильтр определяет сетевой трафик отправитель которого имеет MAC-адрес 0c:c4:7a:7b:8f:e5.	[edit] admin@Edge1# set filter FWTEST-5 rule 10 source mac-address 0c:c4:7a:7b:8f:e5
Создание узла конфигурации для политики межсетевого экранирования FW5 и его правила rule 10. Это правило разрешает трафик, соответствующий указанным критериям.	[edit] admin@Edge1# set policy firewall FW5 rule 10 action accept
Применение фильтра FWTEST-5 к политике межсетевого экрана FW5.	[edit] admin@Edge1# set policy firewall FW5 rule 10 match filter FWTEST-5
Применение политики FW5 ко входящим пакетам на интерфейсе eth1.	[edit] admin@Edge1# set interfaces ethernet eth1 policy in firewall FW5
Фиксация настройки.	[edit] admin@Edge1# commit

20.2.6 Исключение адреса

Правило межсетевого экрана, показанное в примере ниже, разрешает весь трафик из сети 192.168.10.0/24, за исключением того, который предназначен серверу 192.168.20.100.

Для создания политики для исключения адреса выполните следующие действия в режиме настройки:

Пример 175– Исключение адреса

Действие	Команда
Задание параметров фильтра трафика FWTEST-6 – фильтр определяет сетевой трафик отправитель которого имеет ip-адрес из сети 192.168.10.0/24.	[edit] admin@edge# set filter FWTEST-6 rule 10 source address 192.168.10.0/24
Задание параметров фильтра трафика FWTEST-6 – фильтр определяет сетевой трафик, предназначенный для любого узла назначения, КРОМЕ 192.168.20.100. Трафик, не соответствующий правилу, вызывает переход к правилу по умолчанию «**reject all»**.	[edit] admin@edge# set filter FWTEST-6 rule 10 destination address !192.168.20.100
Создание узла конфигурации для политики межсетевого экранирования NEGATED-EXAMPLE и его правила rule 10. Это правило разрешает трафик, соответствующий указанным критериям.	[edit] admin@edge# set policy firewall NEGATED-EXAMPLE rule 10 action accept

Действие	Команда
Применение фильтра FWTEST-6 к политике межсетевого экрана NEGATED-EXAMPLE.	admin@edge# set policy firewall NEGATED-EXAMPLE rule 10 match filter FWTEST-6
Применение политики межсетевого экранирования NEGATED-EXAMPLE ко входящему трафику на eth2.	[edit] admin@edge# set interfaces ethernet eth2 policy in firewall NEGATED-EXAMPLE
Фиксация настройки.	[edit] admin@edge# commit

Вывод настройки.	[edit]
	admin@edge# show policy firewall
	NEGATED-EXAMPLE {
	rule 10 {
	match filter FWTEST-6
	action accept
	}
	} }
	[edit]
	admin@edge# show filter
	FWTEST-6 {
	rule 10 {
	destination {
	address !192.168.20.100
	}
	source {
	address 192.168.10.0/24
	}
	}
	}
	[edit]
	admin@edge# show interfaces ethernet eth2
	address 192.168.10.254/24
	policy {
	in {
	firewall NEGATED-EXAMPLE
	}
	}

20.2.7 Активация в течение указанных периодов времени

Numa Edge поддерживает фильтрацию с учетом даты и времени. Для правил политики межсетевого экранирования существует возможность указать время, которое будет определять период действия правила.

Правило политики межсетевого экранирования, показанное в примере 176, ограничивает время активности правила, настроенного в примере 175, интервалом с 9:00 до 17:00 по рабочим дням. для добавления ограничения к правилу выполните следующие действия в режиме настройки:

Пример 176– Активация в течение указанных периодов времени

Действие	Команда
Установка времени начала действия на 9:00.	[edit] admin@edge# set filter FWTEST-6 rule 10 time starttime 09:00:00
Установка времени окончания действия на 17:00.	[edit] admin@edge# set filter FWTEST-6 rule 10 time stoptime 17:00:00
Установка дней недели.	[edit] admin@edge# set filter FWTEST-6 rule 10 time weekdays Mon,Tue,Wed,Thu,Fri
Фиксация настройки.	[edit] admin@edge# commit
Вывод настройки.	[edit] admin@edge# show policy firewall

Действие	Команда

	NEGATED-EXAMPLE {
	rule 10 {
	match filter FWTEST-6
	action accept
	}
	}
	[edit]
	admin@edge# show filter
	FWTEST-6 {
	rule 10 {
	destination {
	address !192.168.1.100
	}
	source {
	address 192.168.10.0/24
	}
	time {
	starttime 09:00:00
	stoptime 17:00:00
	weekdays Mon,Tue,Wed,Thu,Fri
	} }
	}
	[edit]
	admin@edge# show interfaces ethernet eth2
	address 192.168.10.254/24
	policy {
	in {
	firewall NEGATED-EXAMPLE
	}
	}

20.2.8 Проверка соответствия имен типов ICMP

Межсетевой экран Numa Edge позволяет фильтровать пакеты по именам типов ICMP. Например, для создания правила, разрешающего прохождение пакетов эхо-запросов ICMP на интерфейсе **eth2** межсетевого экрана 'edge' в сторону подсети 192.168.20.0/24, выполните следующие действия в режиме настройки:

Пример 177– Принятие пакетов ICMP с конкретными именами типов

Действие	Команда
Задание параметров фильтра трафика ICMP-NAME – фильтр определяет сетевой трафик, соответствующий протоколу ICMP.	[edit] admin@edge# set filter ICMP-NAME rule 10 protocol icmp
Задание параметров фильтра трафика ICMP-NAME – установка типа пакетов ICMP для проверки совпадения.	[edit] admin@edge# set filter ICMP-NAME rule 10 icmp type echo-request
Создание узла конфигурации для политики межсетевого экранирования FW7 и его правила rule 10. Это правило разрешает трафик, соответствующий указанным критериям.	[edit] admin@edge# set policy firewall FW7 rule 10 action accept
Применение фильтра ICMP-NAME - к политике межсетевого экрана FW7.	[edit] admin@edge# set policy firewall FW7 rule 10 match filter ICMP-NAME
Применение политики FW7 к исходящим пакетам на интерфейсе eth2	[edit] admin@edge# set interfaces ethernet eth2 policy out firewall FW7
Фиксация настройки.	[edit] admin@edge# commit
Вывод настройки.	[edit] admin@edge# show filter ICMP-NAME rule 10 {

Действие	Команда

	icmp {
	type echo-request
	}
	protocol icmp
	}
	[edit]
	admin@edge# show policy firewall FW7
	rule 10 {
	action accept
	match {
	filter ICMP-NAME
	}
	}
	[edit]
	admin@edge# show interfaces ethernet eth2
	address 192.168.20.254/24
	policy {
	out {
	firewall FW7
	}
	}

20.2.9 Ограничение скоростей передачи трафика

Для ограничения скорости прохождения входящих пакетов можно использовать правило политики межсетевого экранирования, включающее фильтр TBF (Token Bucket Filter), работающий по алгоритму маркерного ведра. Частота проходящих пакетов ограничивается административно установленным значением, но возможно ее превышение для небольших групп пакетов в короткий промежуток времени.

Правило политики межсетевого экранирования, показанное в примере 178, ограничивает частоту пакетов эхо-запросов ICMP, настроенных в примере 177, до двух в секунду (но дающего возможность кратковременного превышения этой частоты без игнорирования пакетов).

Для создания политики для ограничения скорости передачи трафика выполните следующие действия в режиме настройки:

Пример 178 – Ограничение скорости для конкретных входящих пакетов

Действие	Команда
Установка требуемой частоты в 2 пакета в секунду.	[edit] admin@edge# set filter ICMP-NAME rule 10 limit packet-rate rate 2/second
Установка размера группы в 5 пакетов.	[edit] admin@edge# set filter ICMP-NAME rule 10 limit packet-rate burst 5
Фиксация настройки.	[edit] admin@edge# commit

Вывод настройки.	[edit]
	admin@edge# show filter ICMP-NAME
	rule 10 {
	icmp {
	type echo-request
	}
	limit {
	packet-rate {
	burst 5
	rate 2/second
	}
	}
	protocol icmp
	}
	[edit]
	admin@edge# show policy firewall

Действие	Команда

	FW7 {
	rule 10 {
	match filter ICMP-NAME
	action accept
	}
	}
	[edit]
	admin@edge# show interfaces ethernet eth2
	address 192.168.20.254/24
	policy {
	out {
	firewall FW7
	}
	}

20.2.10 Проверка соответствия флагов TCP

Numa Edge поддерживает фильтрацию по флагам TCP внутри пакетов TCP. Например, чтобы создать правило для принятия пакетов с установленным флагом SYN и снятыми флагами ACK, FIN и RST, выполните следующие действия в режиме настройки:

Пример 179– Принятие пакетов с установленными конкретными флагами TCP

Действие	Команда
Установка TCP в качестве протокола-образца для проверки совпадения.	[edit] admin@edge# set filter TCP-FLAGS rule 10 protocol tcp
Установка флагов TCP для проверки совпадения.	[edit] admin@edge# set filter TCP-FLAGS rule 10 tcp flags SYN,!ACK,!FIN,!RST
Создание узла конфигурации для политики межсетевого экранирования FW8 и его правила rule 10. Это правило разрешает трафик, соответствующий указанным критериям.	[edit] admin@edge# set policy firewall FW8 rule 10 action accept
Применение фильтра TCP-FLAGS к политике межсетевого экрана FW8.	[edit] admin@edge# set policy firewall FW8 rule 10 match filter TCP-FLAGS
Фиксация настройки.	[edit] admin@edge# commit

Вывод настройки.	[edit]
	admin@edge# show filter TCP-FLAGS
	rule 10 {
	protocol tcp
	tcp {
	flags SYN,!ACK,!FIN,!RST
	}
	}
	[edit]
	admin@edge# show policy firewall
	rule 10 {
	action accept
	match {
	filter TCP-FLAGS
	}
	}

20.2.11 Проверка соответствия групп

Межсетевой экран Numa Edge позволяет определить группы адресов, портов и сетей для осуществления над ними аналогичной фильтрации. Например, для создания правила, отклоняющего трафик на группу адресов и портов из группы сетей, выполните следующие действия в режиме настройки:

Пример 180– Отклонение трафика на основе групп адресов, сетей или портов

Действие	**Команда**
Добавление диапазона адресов в группу адресов.	[edit] admin@# set groups address-group SERVERS address 192.168.10.100-192.168.10.105
Добавление еще одного адреса в группу адресов.	[edit] admin@edge# set groups address-group SERVERS address 192.168.10.107
Добавление сети в группу сетей.	[edit] admin@edge# set groups network-group NETWORKS network 192.168.20.0/24
Добавление порта в группу портов.	[edit] admin@edge# set groups port-group PORTS port 22
Добавление имени порта в группу портов.	[edit] admin@edge# set groups port-group PORTS port ftp
Добавление диапазона портов в группу портов.	[edit] admin@edge# set groups port-group PORTS port 1000-2000
Фиксация настройки.	[edit] admin@edge# commit

Вывод настройки.	[edit]
	admin@edge# show groups
	address-group SERVERS {
	address 192.168.10.100-
	192.168.10.105
	address 192.168.10.107
	}
	[edit]
	admin@edge# show groups
	network-group NETWORKS {
	network 192.168.20.0/24
	}
	[edit]
	admin@edge# show groups
	port-group PORTS {
	port 22
	port ftp
	port 1000-2000
	}

Указание группы адресов получателей в качестве образца для проверки совпадения.	[edit] admin@edge# set filter REJECT-GROUPS rule 10 destination address-group SERVERS
Указание группы портов получателей в качестве образца для проверки совпадения.	[edit] admin@edge# set filter REJECT-GROUPS rule 10 destination port-group PORTS
Указание группы сетей отправителей в качестве образца для проверки совпадения.	[edit] admin@edge# set filter REJECT-GROUPS rule 10 source network-group NETWORKS
Создание узла конфигурации для политики межсетевого экранирования FW10 и его правила rule 10. Это правило запрещает трафик, соответствующий указанным критериям.	[edit] admin@edge# set policy firewall FW10 rule 10 action reject
Применение фильтра REJECT-GROUPS к политике межсетевого экрана FW10.	[edit] admin@edge# set policy firewall FW10 rule 10 match filter REJECT-GROUPS
Фиксация настройки.	[edit] admin@edge# commit

Действие	Команда

Вывод настройки.	[edit]
	admin@edge# show policy firewall FW10
	rule 10 {
	action reject
	match {
	filter REJECT-GROUPS
	}
	}
	[edit]
	admin@edge# show filter REJECT-GROUPS
	rule 10 {
	destination {
	address-group SERVERS
	port-group PORTS
	}
	source {
	network-group NETWORKS
	}
	}

20.2.12 Проверка соответствия недавно встречавшихся отправителей

Команда **recent** может использоваться для предотвращения атак с целью взлома пароля перебором ("brute force"), когда внешнее устройство открывает непрерывный поток подключений (например, к порту SSH) в попытке взломать систему. В таких случаях адрес внешнего отправителя может быть неизвестен; тем не менее, данная команда делает возможным проверку соответствия по поведению внешнего узла без изначальной необходимости в знании его IP-адреса.

Например, для создания правила, ограничивающего число попыток внешних подключений по SSH с одного и того же узла тремя в течение 30 секунд, выполните следующие действия в режиме настройки:

Пример 181 – Игнорирование попыток подключения от одного и того же отправителя при превышении указанного порога их числа за данный промежуток времени

Действие	Команда
Задание параметров фильтра трафика STOP-BRUTE – фильтр определяет сетевой трафик, соответствующий протоколуTCP.	[edit] admin@edge# set filter STOP-BRUTE rule 10 protocol tcp
Проверка порта назначение на совпадение с 22 (т.е. ssh).	[edit] admin@edge# set filter STOP-BRUTE rule 10 destination port 22
Проверка числа попыток подключения.	[edit] admin@edge# set filter STOP-BRUTE rule 10 state new enable
Проверка трехкратного повторения адресов отправителя ...	[edit] admin@edge# set filter STOP-BRUTE rule 10 recent count 3
... в течение 30 секунд.	[edit] admin@edge# set filter STOP-BRUTE rule 10 recent time 30
Создание узла конфигурации для политики межсетевого экранирования FW11 и его правила rule 10. Это правило запрещает трафик, соответствующий указанным критериям.	[edit] admin@edge# set policy firewall FW11 rule 10 action drop
Применение фильтра STOP-BRUTE к политике межсетевого экрана FW11.	[edit] admin@edge# set policy firewall FW11 rule 10 match filter STOP-BRUTE
Фиксация настройки.	[edit] admin@edge# commit
Вывод настройки.	admin@edge# show policy firewall FW11 rule 10 {

Действие	Команда

	action drop
	match {
	filter STOP-BRUTE
	}
	}
	[edit]
	admin@edge# show filter STOP-BRUTE
	rule 10 {
	destination {
	port 22
	}
	protocol tcp
	recent {
	count 3
	time 30
	}
	state {
	new enable
	}
	}

20.3 Просмотр сведений о межсетевом экране

В этом разделе рассматриваются следующие вопросы:

- Вывод сведений о политике межсетевого экранирования.
- Вывод настройки межсетевого экрана на интерфейсах.
- Вывод информации о системных настройках межсетевого экрана.
- В этом разделе есть следующие примеры:
- Пример 182 – Вывод сведений о политиках межсетевого экранирования
- Пример 183 – Вывод конфигурации политики межсетевого экранирования на интерфейсе
- Пример 184 – Отображение узла конфигурации "show policy firewall"

20.3.1 Вывод сведений о политике межсетевого экранирования

Вывести конфигурацию политики межсетевого экранирования можно с помощью команды **policy show firewall** в эксплуатационном режиме, указав имя политики.

В примере ниже выводятся сведения, настроенные для политик межсетевого экранирования FW2 и FW3.

Пример 182 – Вывод сведений о политиках межсетевого экранирования

```
admin@Edge1:~$ policy show firewall FW2
Политика МЭ IPv4 FW2:

 Политика задействована для интерфейсов (eth2.10: out)


rule      pkts      bytes     target    filter
----      ----      -----     ------    ------
10        0         0         ACCEPT    FWTEST-2
default   0         0         DROP

admin@Edge1:~$ policy show firewall FW3
Политика МЭ IPv4 FW3:

 Политика задействована для интерфейсов (eth2: local)


rule      pkts      bytes     target    filter
----      ----      -----     ------    ------
10        0         0         ACCEPT    FWTEST-3
default   0         0         DROP
```

20.3.2 Вывод конфигурации политики межсетевого экранирования на интерфейсе

В примере ниже показано применение политик межсетевого экранирования FW7 межсетевого экрана к интерфейсу eth2.

Пример 183 – Вывод конфигурации политики межсетевого экранирования на интерфейсе

```
admin@Edge1# show interfaces ethernet eth2 policy
   out {
       firewall FW7
   }
```

20.3.3 Вывод конфигурации политики межсетевого экранирования

Всегда можно просмотреть сведения в узлах конфигурации с помощью команды **show** в режиме настройки. В этом случае просмотреть конфигурацию политики межсетевого экранирования можно с помощью команды **show policy firewall** в режиме настройки, как показано в примере :

Пример 184 – Отображение узла конфигурации "show policy firewall"

```
admin@Edge1# show policy firewall FW2
   default-action drop
   rule 10 {
       action accept
       match {
           filter FWTEST-2
       }
   }
```

20.4 Глобальные команды межсетевого экрана

Команды настройки	
system conntrack protocols sip	Установка параметров подсистемы отслеживания состояний соединений для протокола SIP.
system conntrack expect-table-size <размер>	Установка ожидаемого количества отслеживаемых подключений для сетевого фильтра.

system conntrack table-size <размер>	Установка размера таблицы отслеживания подключений для сетевого фильтра.
system conntrack tcp-loose <состояние>	Указание необходимости отслеживания ранее установленных подключений для фильтрации трафика с поддержкой состояния.

20.4.1 system conntrack protocols sip

Установка параметров подсистемы отслеживания состояний соединений для протокола SIP.

Синтаксис

```
set system conntrack protocols sip [enable-indirect-media | enable-indirect-signalling | port <порт>]

delete system conntrack protocols sip [enable-indirect-media | enable-indirect-signalling | port]

show system conntrack protocols sip [port]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
    conntrack {
        protocols {
            sip {
                enable-indirect-media
                enable-indirect-signalling
                port порт
            }
        }
    }
}
```

Параметры

enable-indirect-media

Поддержка непрямых медийных потоков

enable-indirect-signalling

Поддержка непрямых сигнальных соединений

port

Задать номера порта, обрабатывающего трафик SIP. Требует ввода обязательного параметра *порт.*

порт

Номер порта, обрабатывающего трафик SIP.

Значение по умолчанию

Не установлено.

Указания по использованию

Эта команда используется для работы с параметрами подсистемы отслеживания состояний соединений для протокола SIP.

Форма **set** этой команды используется для изменения параметров подсистемы отслеживания состояний соединений для протокола SIP.

Форма **delete** этой команды используется для восстановления значения, принятого по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

20.4.2 system conntrack expect-table-size <размер>

Установка количества ожидаемых связанных подключений для сетевого фильтра.

Синтаксис

```
set system conntrack expect-table-size <размер>
delete system conntrack expect-table-size
show system conntrack expect-table-size
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   conntrack {
      expect-table-size размер   }
}
```

Параметры

размер

Ожидаемое количество отслеживаемых связанных (related) подключений. Диапазон значений от 1 до 50 000 000.

Значение по умолчанию

Ожидаемое количество отслеживаемых связанных (related) соединений, установленное по умолчанию, зависит от размера оперативной памяти устройства и определяется по формуле <размер_оперативной_памяти_кб>/192.

Указания по использованию

Эта команда используется для указания ожидаемого количества отслеживаемых связанных (related) подключений для сетевого фильтра.

Форма **set** этой команды используется для изменения ожидаемого количества отслеживаемых подключений.

Форма **delete** этой команды используется для восстановления значения, принятого по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

20.4.3 system conntrack table-size <размер>

Установка максимального количества отслеживаемых подключений для сетевого фильтра.

Синтаксис

```
set system conntrack table-size <размер>
delete system conntrack table-size
show system conntrack table-size
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   conntrack {
      table-size размер
   }
}
```

Параметры

размер

Максимальное количество отслеживаемых подключений. Диапазон значений от 1 до 50 000 000.

Значение по умолчанию

Максимальное количество отслеживаемых соединений, установленное по умолчанию, зависит от размера оперативной памяти устройства и определяется по формуле <размер_оперативной_памяти_кб>/3.

Указания по использованию

Эта команда используется для указания максимального количества отслеживаемых подключений для сетевого фильтра. Таблица отслеживания подключений для сетевого фильтра служит для отслеживания состояния сетевых подключений и потоков трафика, позволяя системе соотносить их для обеспечения фильтрации трафика с поддержкой состояния.

Форма **set** этой команды используется для изменения максимального количества отслеживаемых подключений.

Форма **delete** этой команды используется для восстановления значения, принятого по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

20.4.4 system conntrack tcp-loose <состояние>

Указание необходимости отслеживания ранее установленных подключений для фильтрации трафика с поддержкой состояния.

Синтаксис

```
set system conntrack tcp-loose <состояние>

delete system conntrack tcp-loose

show system conntrack tcp-loose
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   conntrack {
      tcp-loose состояние
   }
}
```

Параметры

состояние

Указание режима обработки ранее установленных соединений. Допустимые значения:

enable: В системе разрешена обработка ранее установленных подключений;

disable: В системе не разрешена обработка ранее установленных подключений.

Значение по умолчанию

Обработка ранее установленных подключений разрешена.

Указания по использованию

Эта команда используется для указания необходимости применения глобального отслеживания TCP, которая позволяет использовать ранее установленные подключения в фильтрации трафика с поддержкой состояния. При фильтрации трафика с поддержкой состояния система запоминает состояние новых потоков данных, авторизованных из доверенной сети. Если включено глобальное отслеживание подключений TCP, система разрешает прохождение потоков трафика, установленных до отслеживания; если оно отключено, система отклоняет эти потоки.

Форма **set** этой команды используется для указания необходимости разрешения или отклонения ранее установленных подключений.

Форма **delete** этой команд используется для восстановления поведения по умолчанию.

Форма **show** этой команды используется для просмотра настройки глобального отслеживания TCP.

20.5 Команды межсетевого экрана IPv4

Команды настройки	
Команды для интерфейса	
interfaces <интерфейс> policy <направление> firewall <имя_политики>	Применение политики межсетевого экранирования IPv4 к определенному интерфейсу.
Системные настройки	
system ip all-ping <состояние>	Включение или выключение ответа на эхо-запрос IPv4 ICMP (ping).
system ip broadcast-ping <состояние>	Включение или выключение ответа на широковещательные эхо-запросы IPv4 ICMP и запросы метки времени.
system ip log-martians <состояние>	Регистрация пакетов с недопустимыми адресами.
system ip receive-redirects <состояние>	Обработка сообщений IPv4 ICMP о перенаправлении (тип 5).
system ip send-redirects <состояние>	Отправка сообщений IPv4 ICMP о перенаправлении (тип 5).
system ip source-route <состояние>	Обработка пакетов с опциями IP гибкой маршрутизации от источника (Loose Source Route) или жесткой маршрутизации от источника (Strict Source Route)
system ip source-validation <состояние>	Отправка сообщений IPv4 ICMP о перенаправлении (тип 5).
system ip syn-cookies <состояние>	Определение политики для проверки отправителя на основе обратного пути, как определено в RFC 3704.
Группы фильтрации	
groups	Определение группы объектов для ссылки в правилах политики межсетевого экранирования.
groups address-group <имя_группы>	Определение группы IP-адресов для ссылки в правилах политики межсетевого экранирования.
groups address-group <имя_группы> named-list <список>	Указание именованного внешнего списка IP-адресов.
groups domain-group <имя_группы>	Определение группы доменов для ссылки в правилах политики межсетевого экранирования.
groups domain-group <имя_группы> named-list <список>	Указание именованного внешнего списка доменов.
groups network-group <имя_группы>	Определение группы сетей для ссылки в правилах политики межсетевого экранирования.
groups port-group <имя_группы>	Определение группы портов для ссылки в правилах политики межсетевого экранирования.
groups port-group <имя_группы> named-list <список>	Указание именованного внешнего списка портов.
groups user-group <имя_группы>	Определение группы пользователей для ссылки в правилах политики межсетевого экранирования.
Правила и наборы правил (политики межсетевого экранирования)	
policy firewall <имя_политики>	Определение политики межсетевого экранирования IPv4.
policy firewall <имя_политики> default-action <действие>	Установка действия по умолчанию для политики межсетевого экранирования IPv4.
policy firewall <имя_политики> description <описание>	Указание краткого описания для политики межсетевого экранирования IPv4.
policy firewall <имя_политики> enable-default-log	Включение регистрации событий действия по умолчанию.

policy firewall <имя_политики> rule <номер_правила>	Определение правила в политике межсетевого экранирования IPv4.
policy firewall <имя_политики> rule <номер_правила> action <действие>	Указание действия, которое будет применяться к пакетам, для которых было установлено соответствие правилу.
policy firewall <имя_политики> rule <номер_правила> description <описание>	Указание краткого описания для правила в политике межсетевого экранирования IPv4.
policy firewall <имя_политики> rule <номер_правила> log <состояние>	Включение/выключение регистрации событий фильтрации трафика для указанного правила указанной политики.
policy firewall <имя_политики> rule <номер_правила> match filter <фильтр>	Задание фильтра, который будет использоваться для выборки пакетов для указанного правила указанной политики.
Эксплуатационные команды	
policy clear firewall <имя_политики>	Очистка статистики для политики межсетевого экранирования.
policy clear firewall <имя_политики> rule <номер_правила>	Очистка статистики для указанного правила политики межсетевого экранирования.
policy clear firewall <имя_политики> rule <номер_правила> filter	Очистка статистики для фильтра, связанного с указанным правилом политики межсетевого экранирования IPv4-трафика.
policy clear firewall <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>	Очистка статистики для указанного правила фильтра, связанного с указанным правилом политики межсетевого экранирования IPv4-трафика.
policy show firewall <имя_политики>	Вывод сведений и статистики для указанной политики межсетевого экранирования IPv4-трафика.
policy show firewall <имя_политики> rule <номер_правила>	Вывод сведений и статистики для указанного правила политики межсетевого экранирования Ipv4-трафика.
policy show firewall <имя_политики> rule <номер_правила> filter	Вывод сведений и статистики по фильтру для указанного правила политики межсетевого экранирования IPv4.
named-list <тип_списка> export <имя_списка> to <имя_файла>	Экспорт именованных списков.
named-list <тип_списка> import <имя_списка> from <имя_файла>	Импорт именованных списков.
named-list <тип_списка> remove <имя_списка>	Удаление именованных списков.
named-list <тип_списка> show	Отображение перечня именованных списков определенного типа, присутствующих в системе.

20.5.1 interfaces <интерфейс> policy <направление> firewall <имя_политики>

Применение политики межсетевого экранирования к определенному интерфейсу.

Синтаксис

```
set interfaces <интерфейс> policy <направление>  firewall <имя_политики>
delete interfaces <интерфейс> policy <направление>  firewall <имя_политики>
show interfaces <интерфейс> policy <направление>  firewall <имя_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
    policy {
        направление {
            firewall имя_политики
        }
    }
```

```
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже в разделе Указания по использованию.

направление

Обязательный. Направление трафика, к которому применяется политика межсетевого экранирования. Допустимые значения указаны в таблице ниже:

Таблица 157 – Направления трафика

Значение	Описание
in	Транзитный трафик, принимаемый на указанном интерфейсе
out	Транзитный трафик, отправляемый с указанного интерфейса
local	Трафик, принятый на интерфейсе, предназначенный для локальной системы.

имя_политики

Имя политики межсетевого экранирования.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет применить политику межсетевого экранирования к интерфейсу.

Фильтрация транзитного трафика или трафика, предназначенного для локальной системы, не осуществляется до тех пор, пока политика межсетевого экранирования не будет применена к интерфейсу (реальному или виртуальному) с использованием данной команды.

Для включения межсетевого экранирования следует определить политику с помощью команды **policy firewall**. Затем следует применить политику к интерфейсам и/или виртуальным интерфейсам, используя данную команду. После чего указанная политика межсетевого экранирования будет функционировать в качестве пакетного фильтра.

На каждом интерфейсе можно применить до трех политик межсетевого экранирования: одну как фильтр транзитного трафика, принимаемого на интерфейсе (in), одну – как фильтр транзитного трафика, покидающего интерфейс (out) и одну – как фильтр трафика, предназначенного для локальной системы (local).

В приведенной ниже таблице показаны типы поддерживаемых интерфейсов и синтаксис.

Таблица 158 – Типы интерфейсов

Тип интерфейса	Синтаксис
Агрегирование каналов	bonding bondx
Виртуальный интерфейс агрегированных каналов	bonding bondx vif идентификатор_vlan
Сетевой мост	bridge brx
Ethernet	ethernet ethx
Ethernet PPPoE	ethernet ethx pppoe номер
Виртуальный интерфейс Ethernet	ethernet ethx vif идентификатор_vlan
Ethernet Vif PPPoE	ethernet ethx vif идентификатор_vlan pppoe номер
Интерфейс заглушки	loopback lo
Многоканальная связь	multilink mlx
OpenVPN	openvpn vtunx
Псевдо-Ethernet	pseudo-ethernet pethx
Последовательный интерфейс	serial srx vif идентификатор_vlan
Туннель	tunnel tunx

Форма **set** данной команды позволяет применить политику межсетевого экранирования к интерфейсу.

Форма **delete** данной команды позволяет удалить политику межсетевого экранирования для интерфейса.

Форма **show** данной команды используется для отображения конфигурации политики межсетевого экранирования на интерфейсе.

20.5.2 system ip all-ping <состояние>

Включение или выключение обработки ответа на эхо-запросы IPv4 ICMP (ping).

Синтаксис

```
set system ip all-ping <состояние>
delete system ip all-ping
show system ip all-ping
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system ip {
   all-ping состояние
}
```

Параметры

состояние

Параметр обработки ответов на эхо-запросы IPv4 ICMP. Допустимые значения:

enable: Система будет обрабатывать эхо-запросы IPv4 ICMP;

disable: Система не будет обрабатывать эхо-запросы IPv4 ICMP.

Значение по умолчанию

По умолчанию разрешена обработка эхо-запросов IPv4 ICMP.

Указания по использованию

Данная команда позволяет разрешить или запретить обработку эхо-запросов IPv4 ICMP (ping).

Действие распространяется на все типы таких сообщений: одноадресные, широковещательные или многоадресные. Эхо-запросы IPv4 ICMP позволяют проверить доступность устройства для локальной системы. Такие сообщения часто запрещают, так как они могут быть использованы для проведения атак отказа в обслуживании (Denial of Service (DoS) attacks).

Форма **set** данной команды используется для включения или отключения ответов на эхо-запросы IPv4 ICMP.

Форма **delete** данной команды используется для восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки обработки эхо-запросов IPv4 ICMP.

20.5.3 system ip broadcast-ping <состояние>

Включение или выключение ответа на широковещательные эхо-запросы IPv4 ICMP и запросы метки времени.

Синтаксис

```
set system ip broadcast-ping <состояние>
delete system ip broadcast-ping
show system ip broadcast-ping
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system ip {
```

```
    broadcast-ping состояние
}
```

Параметры

состояние

Параметр обработки ответов на широковещательные эхо-запросы IPv4 ICMP и запросы метки времени. Допустимые значения:

enable: Система будет обрабатывать широковещательные эхо-запросы IPv4 ICMP и запросы метки времени;

disable: Система не будет обрабатывать широковещательные эхо-запросы IPv4 ICMP и запросы метки времени.

Значение по умолчанию

По умолчанию эхо-запросы IPv4 ICMP и запросы метки времени не обрабатываются.

Указания по использованию

Данная команда позволяет разрешить или запретить обработку широковещательных эхо-запросов IPv4 ICMP и широковещательных запросов метки времени IPv4 ICMP.

Эхо-запросы IPv4 ICMP позволяют проверить доступность устройства для локальной системы. Эхо-запросы ICMP, особенно широковещательные, часто запрещают, так как они могут быть использованы для проведения атак отказа в обслуживании (Denial of Service (DoS) attacks). Запрос метки времени позволяет запросить текущую дату и время у другого устройства. Широковещательные запросы метки времени также часто запрещают, так как они могут использоваться для проведения атак отказа в обслуживании, а также из-за того, что они позволяют злоумышленнику узнать дату и время, установленное на устройстве.

Форма **set** данной команды позволяет указать, следует ли отвечать на широковещательные эхо-запросы ICMP IPv4 и запросы метки времени.

Форма **delete** данной команды используется для восстановления поведения по умолчанию для обработки таких сообщений.

Форма **show** данной команды используется для отображения настройки.

20.5.4 system ip log-martians <состояние>

Регистрация пакетов с недопустимыми адресами.

Синтаксис

```
set system ip log-martians <состояние>
delete system ip log-martians
show system ip log-martians
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system ip {
    log-martians состояние
}
```

Параметры

состояние

Параметр регистрации пакетов с недопустимыми адресами. Допустимые значения:

enable: Система будет регистрировать пакеты с недопустимыми адресами;

disable: Система не будет регистрировать пакеты с недопустимыми адресами.

Значение по умолчанию

Регистрация сетевых пакетов с недопустимыми адресами включена.

Указания по использованию

Данная команда позволяет включить или отключить регистрацию в журнале пакетов с недопустимыми адресами.

Форма **set** данной команды позволяет включить или выключить регистрацию пакетов с недопустимыми адресами.

Форма **delete** данной команды позволяет восстановить поведение по умолчанию для регистрации пакетов с недопустимыми адресами.

Форма **show** данной команды используется для отображения настройки.

20.5.5 system ip receive-redirects <состояние>

Обработка полученных пакетов перенаправлений IPv4 ICMP (тип 5).

Синтаксис

```
set system ip receive-redirects <состояние>
delete system ip receive-redirects
show system ip receive-redirects
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system ip {
   receive-redirects состояние
}
```

Параметры

состояние

Параметр обработки полученных пакетов перенаправлений IPv4 ICMP (тип 5). Допустимые значения:

enable: Система будет обрабатывать полученные пакетов перенаправлений IPv4 ICMP (тип 5);

disable: Система не будет обрабатывать полученные пакеты перенаправлений IPv4 ICMP (тип 5).

Значение по умолчанию

По умолчанию обработка полученных пакетов перенаправлений IPv4 ICMP (тип 5) не производится.

Указания по использованию

Данная команда позволяет разрешить или запретить прием сообщений IPv4 ICMP о перенаправлении (тип 5). Сообщения ICMP о перенаправлении могут позволить произвольному отправителю подделывать пакеты и изменять системную таблицу маршрутизации. Таким образом, система может быть уязвима по отношению к атаке "человек посередине".

Форма **set** позволяет разрешить или запретить прием сообщений IPv4 ICMP о перенаправлении.

Форма **delete** используется для удаления установленного значения.

Форма **show** данной команды используется для отображения установленного значения.

20.5.6 system ip send-redirects <состояние>

Обработка исходящих пакетов IPv4 ICMP о перенаправлении (тип 5).

Синтаксис

```
set system ip send-redirects <состояние>
delete system ip send-redirects
show system ip send-redirects
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system ip {
   send-redirects состояние
}
```

Параметры

состояние

Параметр обработки исходящих пакетов перенаправлений IPv4 ICMP. Допустимые значения:

enable: Система будет посылать пакеты перенаправлений IPv4 ICMP (тип 5);

disable: Система не будет посылать пакеты перенаправлений IPv4 ICMP (тип 5).

Значение по умолчанию

По умолчанию отправка пакетов перенаправлений IPv4 ICMP (тип 5) разрешена.

Указания по использованию

Данная команда позволяет разрешить или запретить отправку сообщений IPv4 ICMP о перенаправлении. Отправка сообщений redirect потенциально может изменить таблицу маршрутизации узла или маршрутизатора, которому предназначено сообщение.

Форма **set** данной команды позволяет разрешить или запретить отправку сообщений IPv4 ICMP о перенаправлении.

Форма **delete** данной команды позволяет удалить указанное значение.

Форма **show** позволяет отобразить указанное значение.

20.5.7 system ip source-route <состояние>

Обработка пакетов с опциями IP гибкой маршрутизации от источника (Loose Source Route) или жесткой маршрутизации от источника (Strict Source Route).

Синтаксис

```
set system ip source-route <состояние>
delete system ip source-route
show system ip source-route
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system ip {
   source-route состояние
}
```

Параметры

состояние

Параметр обработки пакетов с опциями IP маршрутизации от источника. Допустимые значения:

enable: Система будет обрабатывать пакеты с установленными опциями IP маршрутизацией от источника;

disable: Система не будет обрабатывать пакеты с установленными опциями IP маршрутизацией от источника.

Значение по умолчанию

По умолчанию пакеты с установленными опциями IP маршрутизацией от источника не обрабатываются.

Указания по использованию

Данная команда позволяет разрешить или запретить пакеты с установленными опциями гибкой или жесткой маршрутизации от источника.

Маршрутизация от источника разрешает приложениям указать один или несколько промежуточных адресов получателя для исходящих пакетов в обход таблицы маршрутизации. Данная возможность в некоторых случаях используется для выявления неисправностей, но делает сеть уязвимой к атакам, при которых сетевой трафик перенаправляется через централизованную точку записи трафика.

Форма **set** данной команды позволяет запретить или разрешить обработку опций IP маршрутизации от источника.

Форма **delete** данной команды используется для восстановления поведения по умолчанию для обработки опций маршрутизации от источника.

Форма **show** данной команды используется для отображения настройки.

20.5.8 system ip source-validation <состояние>

Определение политики для проверки отправителя на основе обратного пути, как определено в RFC 3704.

Синтаксис

```
set system ip source-validation <состояние>

delete system ip source-validation

show system ip source-validation
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system ip {
   source-validation состояние
}
```

Параметры

состояние

Параметр определения политики проверки пакетов отправителя на основе обратного пути. Допустимые значения представлены в таблице ниже.

Таблица 159 – Состояние. Значения.

Значение	Описание
disable	Проверка отправителя на основе обратного пути не производится.
loose	Используется пересылка по гибкому обратному пути (Loose Reverse Path Forwarding), как определено в RFC3704.
strict	Используется пересылка по жесткому обратному пути (Strict Reverse Path Forwarding), как определено в RFC3704.

Значение по умолчанию

По умолчанию проверка отправителя на основе обратного пути не производится.

Указания по использованию

Данная команда используется для определения политики для проверки отправителя на основе обратного пути, как определено в RFC3704.

Форма **set** данной команды используется для указания политики проверки отправителя на основе обратного пути, как указано в RFC3704.

Форма **delete** данной команды позволяет удалить установленное значение.

Форма **show** позволяет отобразить установленное значение.

20.5.9 system ip syn-cookies <состояние>

Использование определенного способа формирования номера последовательности TCP SYN для предотвращения атак SYN-flood (одна из разновидностей сетевых атак отказа в обслуживании, которая

заключается в отправке большого количества SYN-запросов (запросов на подключение по протоколу TCP) в достаточно короткий период времени).

Синтаксис

```
set system ip syn-cookies <состояние>

delete system ip syn-cookies

show system ip syn-cookies
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system ip {
   syn-cookies состояние
}
```

Параметры

состояние

Параметр использования определенного способа формирования номера последовательности TCP SYN. Допустимые значения:

enable: Включение механизма предотвращения атак, на основе формирования определенного номера последовательности;

disable: Отключение механизма предотвращения атак, на основе формирования определенного номера последовательности.

Значение по умолчанию

По умолчанию механизм предотвращения атак, на основе формирования определенного номера последовательности включен.

Указания по использованию

Данная команда позволяет включить или отключить механизм предотвращения атак, на основе формирования определенного номера последовательности. Включение данной опции позволит защитить систему от атак отказа в обслуживании, заключающихся в отправке большого количества SYN-запросов (запросов на подключение по протоколу TCP) в короткий срок. При установлении соединения TCP, отправитель посылает пакет SYN (синхронизация). Получатель возвращает пакет SYN ACK (подтверждение синхронизации). После чего отправитель посылает пакет ACK (подтверждение), и соединение считается установленным. Данная последовательность действий называется “тройным рукопожатием TCP”.

После того как получатель отправляет пакет SYN ACK, соединение добавляется в очередь для соединений, ожидающих окончания установления. Злоумышленник может заполнить очередь подключений поддельными пакетами TCP SYN, от различных IP-адресов. После того как очередь подключений будет полностью заполнена, произойдет отказ в обслуживании сервисов TCP.

При включении этой опции вместо добавления соединения в очередь для соединений, получатель отправляет пакет SYN ACK с номером последовательности, созданным по определенному алгоритму, использующему криптографическую хеш-функцию от IP-адреса отправителя, номера порта и других сведений. Пакет ACK, который присылает в ответ отправитель включает в себя этот номер последовательности, который затем проверяется получателем. Таким образом, получатель выделяет память только при получении третьего пакета «рукопожатия TCP», а не после первого, как происходит обычно. Однако, следует учесть, что используемая криптографическая хеш-функция требует выделения ресурсов системы, и в том случае если ожидается большое количество входящих подключений, следует использовать эту опцию с осторожностью.

Форма **set** данной команды позволяет включить или отключить механизма предотвращения атак, на основе формирования определенного номера последовательности.

Форма **delete** данной команды позволяет восстановить значение, принятое по умолчанию.

Форма **show** данной команды позволяет отобразить настройку.

20.5.10 groups

Определение группы объектов для ссылки в правилах политики межсетевого экранирования.

Синтаксис

```
set groups
delete groups
show groups
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
groups {
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет определить группу объектов, на основе которой будет производиться фильтрация пакетов. Группы фильтрации позволяют группировать различные сетевые объекты, и устанавливать соответствие для сетевого пакета при совпадении с любым элементом группы, что позволяет не указывать элементы по отдельности. Могут быть созданы группы адресов, сетей или интерфейсов.

Форма **set** данной команды используется для создания настройки группы фильтрации.

Форма **delete** данной команды используется для удаления группы фильтрации.

Форма **show** данной команды используется для отображения настройки группы фильтрации.

20.5.11 groups address-group <имя_группы>

Определение группы IP-адресов для ссылки в правилах политики межсетевого экранирования.

Синтаксис

```
set groups address-group <имя_группы> [address <адрес> | description описание]
delete groups address-group <имя_группы> [address [<адрес>] | description]
show groups address-group <имя_группы> [address | description]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
groups {
   address-group имя_группы {
      address адрес
      description описание
   }
}
```

Параметры

имя_группы

Обязательный. Имя группы адресов.

адрес

IPv4-адрес. Добавление указанного IPv4-адреса, диапазона IPv4-адресов или сетей IPv4 в указанную группу. Допустимые значения представлены в таблице ниже:

Таблица 160 – Формат указания адресов в составе address-group

Значение	Описание
<x.x.x.x>	Адрес IPv4
<x.x.x.x>-<x.x.x.x>	Диапазон адресов IPv4
<x.x.x.x/x>	Сеть IPv4

описание

Позволяет указать краткое описание для группы адресов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания группы адресов. Группа адресов представляет собой набор IP-адресов, диапазонов IP-адресов или сетей IPv4 на которую можно указать ссылку в правиле политики межсетевого экранирования.

Соответствие группе адресов устанавливается в том случае, если адрес пакета совпадает с любым адресом или диапазоном адресов, входящих в группу.

Форма **set** данной команды используется для указания группы адресов.

Форма **delete** данной команды используется для удаления группы адресов или элемента группы.

Форма **show** данной команды используется для отображения настройки группы адресов.

ПРИМЕЧАНИЕ Для любой группы адреса задаются либо указанием отдельного адреса, диапазона адресов или сетей данной командой, либо указанием списка адресов командой groups address-group <имя_группы> named-list <список>. Параллельное использование обоих механизмов не допускается.

20.5.12 groups address-group <имя_группы> named-list <список>

Указание именованного внешнего списка адресов.

Синтаксис

```
set groups address-group <имя_группы> named-list <список>
delete groups address-group <имя_группы> named-list [<список>]
show groups address-group <имя_группы> named-list
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
groups {
   address-group имя_группы {
      named-list список
   }
}
```

Параметры

имя_группы

Обязательный. Имя группы адресов.

список

Имя списка адресов. Для работы с внешними списками адресов используются команды эксплуатационного режима **named-list address**.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания списка адресов.

Форма **set** данной команды используется для указания именованного списка адресов.

Форма **delete** данной команды используется для удаления именованного списка адресов.

Форма **show** данной команды используется для отображения настройки именованного списка адресов.

ПРИМЕЧАНИЕ Для любой группы адреса задаются либо указанием списка адресов данной командой, либо указанием отдельного адреса (диапазона адресов или сетей) командой groups address-group <имя_группы>. Параллельное использование обоих механизмов не допускается.

20.5.13 groups domain-group <имя_группы>

Определение группы доменов для ссылки в правилах политики межсетевого экранирования.

Синтаксис

```
set groups domain-group <имя_группы> [domain <домен> | description <описание>]
delete groups domain-group <имя_группы> [domain [<домен>] | description]
show groups domain-group <имя_группы> [domain | description]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
groups {
   domain-group имя_группы {
      domain домен
      description описание
   }
}
```

Параметры

имя_группы

Обязательный. Имя группы доменов.

домен

Добавление указанного доменного имени в группу. Используется текстовый формат.

описание

Позволяет указать краткое описание для группы доменов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания группы доменов.

Соответствие группе доменов устанавливается в том случае, если адрес пакета совпадает с любым адресом или диапазоном адресов, входящих в группу.

Форма **set** данной команды используется для указания группы доменов.

Форма **delete** данной команды используется для удаления группы доменов или элемента группы.

Форма **show** данной команды используется для отображения настройки группы доменов.

ПРИМЕЧАНИЕ Для любой группы домены задаются либо указанием отдельного домена данной командой, либо указанием списка доменов командой groups domain-group <имя_группы> named-list <список>. Параллельное использование обоих механизмов не допускается.

20.5.14 groups domain-group <имя_группы> named-list <список>

Указание именованного внешнего списка доменов.

Синтаксис

```
set groups domain-group <имя_группы> named-list <список>
delete groups domain-group <имя_группы> named-list [<список>]
show groups domain-group <имя_группы> named-list
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
groups {
   domain-group имя_группы {
      named-list список
   }
}
```

Параметры

имя_группы

Обязательный. Имя группы доменов.

список

Имя списка доменов. Для работы с внешними списками доменов используются команды эксплуатационного режима **named-list domain**.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания именованного списка доменов.

Форма **set** данной команды используется для указания именованного списка доменов.

Форма **delete** данной команды используется для удаления именованного списка доменов.

Форма **show** данной команды используется для отображения настройки именованного списка доменов.

ПРИМЕЧАНИЕ Для любой группы домены задаются либо список доменов командой groups domain-group <имя_группы>, либо именованный список. Параллельное использование обоих механизмов не допускается.

20.5.15 groups network-group <имя_группы>

Данный узел команд присутствует в системе для обеспечения обратной совместимости со старыми версиями оборудования. Вместо него следует использовать функционал **groups address-group**. Данный узел может быть удален с дальнейшими обновлениями.

20.5.16 groups port-group <имя_группы>

Определение группы портов для ссылки в фильтрах сетевого трафика.

Синтаксис

```
set groups port-group <имя_группы> [port <порт> | description <описание>]
delete groups port-group <имя_группы> [port [<порт>] | description]
show groups port-group <имя_группы> [port | description]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
groups {
   port-group имя_группы {
      description описание
      port порт
   }
}
```

Параметры

имя_группы

Обязательный. Имя группы портов.

порт

Добавление номера порта в указанную группу портов. Допустимые значения представлены в таблице ниже:

Таблица 161 – Формат указания портов в составе port-group

Значение	Описание
<text>	Имя порта (любое из файла /etc/services)
<0-65535>	Номер порта
<start>-<end>	Диапазон портов

описание

Позволяет указать краткое описание для группы портов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания группы портов. Группа портов представляет собой набор имен портов, номеров портов и диапазонов портов, что позволяет после определения группы указать одну ссылку на все ее элементы в правиле политики межсетевого экранирования.

Соответствие группе портов устанавливается в том случае, если порт сетевого пакета совпадает с любым именем или номером сетевого порта, входящего в группу.

Форма **set** данной команды используется для указания группы портов.

Форма **delete** данной команды используется для удаления группы портов или ее элементов.

Форма **show** данной команды используется для отображения настройки группы портов.

ПРИМЕЧАНИЕ Для любой группы портов задаются либо перечень портов данной командой, либо именованный список командой groups port-group <имя_группы> named-list <список>. Параллельное использование обоих механизмов не допускается.

20.5.17 groups port-group <имя_группы> named-list <список>

Определение группы портов для ссылки в правилах фильтров сетевого трафика.

Синтаксис

```
set groups port-group <имя_группы> named-list <список>
delete groups port-group <имя_группы> named-list [<список>]
show groups port-group <имя_группы> named-list
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
groups {
   port-group имя_группы {
      named-list список
   }
}
```

Параметры

имя_группы

Обязательный. Имя группы портов.

список

Имя списка группы портов. Для работы с внешними списками доменов используются команды эксплуатационного режима **named-list port**.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания именованного списка группы портов.

Форма **set** данной команды используется для указания именованного списка сетей.

Форма **delete** данной команды используется для удаления именованного списка сетей.

Форма **show** данной команды используется для отображения настройки именованного списка сетей.

ПРИМЕЧАНИЕ Для любой группы портов задаются либо перечень портов командой groups port-group <имя_группы>, либо именованный список портов данной командой. Параллельное использование обоих механизмов не допускается.

20.5.18 groups user-group <имя_группы>

Определение группы пользователей для ссылки в фильтрах сетевого трафика.

Синтаксис

```
set groups user-group <имя_группы> [user <имя_пользователя> | ttl <время>]
delete groups user-group <имя_группы> [user [<имя_пользователя>] | ttl]
show groups user-group <имя_группы> [user | ttl]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
groups {
   user-group имя_группы {
```

```
        ttl время
        user имя_пользователя
    }
}
```

Параметры

имя_группы

Обязательный. Имя группы пользователей.

user

Добавление имени пользователя в указанную группу пользователей. Для указания имени пользователя используется текстовый формат.

время

Указывает период времени после успешной авторизации, в течение которого IPv4 адрес считается соответствующим указанному пользователю. Диапазон допустимых значений составляет от 1 до 86400 секунд.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания группы пользователей. Группа пользователей представляет собой набор имен пользователей, что позволяет после определения группы указать одну ссылку на все ее элементы в правиле политики межсетевого экранирования.

Соответствие группе пользователей устанавливается в том случае, если пользователь, успешно прошедший авторизацию, входит в группу.

Форма **set** данной команды используется для указания группы пользователей.

Форма **delete** данной команды используется для удаления группы пользователей или ее элементов.

Форма **show** данной команды используется для отображения настройки группы пользователей.

20.5.19 policy firewall <имя_политики>

Определение политики межсетевого экранирования.

Синтаксис

```
set policy firewall <имя_политики>
delete policy firewall [<имя_политики>]
show policy firewall [<имя_политики>]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    firewall {
        имя_политики {
        }
    }
}
```

Параметры

имя_политики

Множественный узел. Текст. Имя политики межсетевого экранирования. Можно определить несколько политик межсетевого экранирования IPv4, создав соответствующее количество узлов конфигурации.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет определить политику межсетевого экранирования IPv4. Политика может включать в себя до 65535 правил.

Форма **set** данной команды используется для создания и изменения политики межсетевого экранирования.

Форма **delete** данной команды используется для удаления политики межсетевого экранирования.

Форма **show** данной команды используется для отображения конфигурации политики межсетевого экранирования.

20.5.20 policy firewall <имя_политики> default-action <действие>

Установка действия по умолчанию для набора правил IPv4.

Синтаксис

```
set policy firewall <имя_политики> default-action <действие>
delete policy firewall <имя_политики> default-action
show policy firewall <имя_политики> default-action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    firewall {
        имя_политики {
            default-action действие
        }
    }
}
```

Параметры

имя_политики

Имя политики межсетевого экранирования.

действие

Действие по умолчанию, которое осуществляется в том случае, если для политики не было установлено ни одного соответствия. Допустимые значения представлены в таблице ниже.

Таблица 162 – Действия по умолчанию для политик межсетевого экранирования.

Значение	Описание
accept	Принять пакет
drop	Отбросить пакет без уведомления
reject	Отбросить пакет и отправить сообщение ICMP с уведомлением хосту, пославшему пакет

Значение по умолчанию

В том случае если действие по умолчанию явно не указано, если для пакета не было установлено ни одного соответствия правилам политики, пакет отбрасывается без уведомления.

Указания по использованию

Данная команда позволяет указать действие по умолчанию, которое будет выполняться в том случае, если для пакета не было установлено ни одного соответствия правилам политики.

В том случае если для пакета не было установлено соответствие ни одному правилу в политике, к нему применяется действие, принятое по умолчанию. По умолчанию, пакет отбрасывается без отправки сообщения ICMP с уведомлением о том, что адресат недоступен.

Форма **set** данной команды позволяет установить действие по умолчанию для политики межсетевого экранирования.

Форма **delete** данной команды используется для восстановления поведения по умолчанию для пакетов, для которых не было установлено ни одного соответствия критериям правила.

Форма **show** данной команды используется для отображения настройки политики по умолчанию.

20.5.21 policy firewall <имя_политики> description <описание>

Указание краткого описания для политики межсетевого экранирования IPv4.

Синтаксис

```
set policy firewall <имя_политики> description <описание>
delete policy firewall <имя_политики> description
show policy firewall <имя_политики> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   firewall {
      имя_политики {
         description описание
      }
   }
}
```

Параметры

имя_политики

Имя политики межсетевого экранирования.

описание

Описание политики межсетевого экранирования. В том случае если описание содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать описание для политики межсетевого экранирования.

Форма **set** данной команды используется для создания и изменения описания.

Форма **delete** используется для удаления описания.

Форма **show** используется для отображения настройки описания.

20.5.22 policy firewall <имя_политики> enable-default-log

Указание краткого описания для политики межсетевого экранирования IPv4.

Синтаксис

```
set policy firewall <имя_политики> enable-default-log
delete policy firewall <имя_политики> enable-default-log
```

```
show policy firewall <имя_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    firewall {
        имя_политики {
            enable-default-log
        }
    }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет включить регистрацию событий для действия по умолчанию указанной политики межсетевого экранирования.

Форма **set** данной команды используется для включения регистрации событий для действия по умолчанию указанной политики межсетевого экранирования.

Форма **delete** используется для отключения регистрации событий для действия по умолчанию указанной политики межсетевого экранирования.

Форма **show** используется для отображения настройки.

20.5.23 policy firewall <имя_политики> rule <номер_правила>

Определение правила в политике межсетевого экранирования IPv4.

Синтаксис

```
set policy firewall <имя_политики> rule <номер_правила>
delete policy firewall <имя_политики> rule [<номер_правила>]
show policy firewall <имя_политики> rule [<номер_правила>]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    firewall {
        имя_политики {
            rule номер_правила {
            }
        }
    }
}
```

Параметры

имя_политики

Имя политики межсетевого экранирования.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65 535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет определить правило в политике межсетевого экранирования. Политика может включать в себя до 65 535 настраиваемых правил.

Правила политики исполняются в порядке следования их номеров, от наименьшего к наибольшему. Напрямую изменить номер правила нельзя, так как он является идентификатором узла конфигурации; однако, можно изменять номера правил при помощи команды **rename**.

Для того чтобы не прибегать к изменению номеров правил, хорошей практикой является указание номеров с шагом 10. Это позволяет оставить пространство, куда можно будет впоследствии добавить новые правила.

Форма **set** данной команды используется для создания или изменения правила в политике межсетевого экранирования.

Форма **delete** данной команды используется для удаления правила из политики межсетевого экранирования.

Форма **show** данной команды используется для отображения настройки правила политики межсетевого экранирования.

20.5.24 policy firewall <имя_политики> rule <номер_правила> action <действие>

Указание действия, которое будет применяться к пакетам, для которых было установлено соответствие правилу.

Синтаксис

```
set policy firewall <имя_политики> rule <номер_правила> action <действие>
delete policy firewall <имя_политики> rule <номер_правила> action
show policy firewall <имя_политики> rule <номер_правила> action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    firewall {
        имя_политики {
            rule номер_правила {
                action действие
            }
        }
    }
}
```

Параметры

имя_политики

Имя политики межсетевого экранирования.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65 535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

действие

Действие, которое будет выполнено, в том случае если пакет удовлетворяет критериям, указанным в правиле. Допустимые значения представлены в таблице ниже.

Таблица 163 – Действия для правил политик межсетевого экранирования.

Значение	Описание
accept	Принять пакет
delude	В ответ на сообщение с установленным флагом SYN будет отправлено сообщение с флагами SYN-ACK, но в остальных случаях отправляется сообщение с флагом RST. Таким образом создается видимость того, что порт открыт и принимает подключения.
drop	Отбросить пакет без уведомления
inspect	Пересылка пакета, для которого было установлено соответствие системе предотвращения вторжений (IPS). Система предотвращения вторжений при этом должна быть включена. (При наличии сервиса idps)
reject	Отбросить пакет и отправить сообщение ICMP с уведомлением хосту, пославшему пакет
tarpit	При указании этого действия, в случае получения запроса на соединение, оно будет установлено, после чего размер окна будет установлен равным нулю, что вынудит систему, отправившую запрос на соединение, прекратить передачу данных. Любые попытки закрыть соединение игнорируются, таким образом соединение остается открытым, пока не истечет срок таймаута, что повлечет расходование локальных ресурсов системы, инициировавшей подключение, но не ресурсов Numa Edge (за исключением ресурсов системы отслеживания соединений, если она используется в МЭ).

Значение по умолчанию

Пакеты отбрасываются.

Указания по использованию

Данная команда позволяет указать действие, которое будет применено к пакетам, для которых было установлено соответствие критериям, указанным в правиле. В правиле может быть указано только одно действие.

Форма **set** данной команды используется для указания действия, которое будет применяться к пакетам, для которых установлено соответствие критериям правила.

Форма **delete** данной команды позволяет восстановить действие, принятое по умолчанию.

Форма **show** данной команды используется для отображения настройки действия для правила политики межсетевого экранирования.

20.5.25 policy firewall <имя_политики> rule <номер_правила> description <описание>

Указание краткого описания для политики межсетевого экранирования IPv4.

Синтаксис

```
set policy firewall <имя_политики> rule <номер_правила> description <описание>

delete policy firewall <имя_политики> rule <номер_правила> description

show policy firewall <имя_политики> rule <номер_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    firewall {
```

```
        имя_политики {
            rule номер_правила {
                description описание
            }
        }
    }
}
```

Параметры

имя_политики

Имя политики межсетевого экранирования.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65 535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

описание

Описание правила в политике межсетевого экранирования. В том случае если описание содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать описание правила в политике межсетевого экранирования.

Форма **set** данной команды используется для создания и изменения описания.

Форма **delete** используется для удаления описания.

Форма **show** используется для отображения настройки описания.

20.5.26 policy firewall <имя_политики> rule <номер_правила> log <состояние>

Включение/выключение регистрации событий фильтрации трафика для указанного правила указанной политики.

Синтаксис

```
set policy firewall <имя_политики> rule <номер_правила> log <состояние>
delete policy firewall <имя_политики> rule <номер_правила> log
show policy firewall <имя_политики> rule <номер_правила> log
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    firewall {
        имя_политики {
            rule номер_правила {
                log состояние
            }
        }
    }
```

}

Параметры

имя_политики

Имя определённой политики фильтрации трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

состояние

Указывает режим регистрации событий для правил политики. Допустимые значения:

enable: Включение регистрации событий фильтрации для правила политики;

disable: Отключение регистрации событий фильтрации для правила политики.

Значение по умолчанию

Отсутствует.

Указания по использованию

Включает или отключает журналирование событий для правила политики.

В том случае, если задействовано журналирование для правила политики, в системный лог (журнал) будут выводиться сообщения для всех пакетов, подпадающих под правило.

Для каждого сообщения формируется префикс в квадратных скобках вида **[f-<имя_политики>-<номер правила>-<действие>].**

Имя политики может быть записано в журнале не полностью в связи с системным ограничением общей длины префикса в 29 символов. Действия в файле журнала кодируются следующими аббревиатурами:

Таблица 164 – Аббревиатуры действий правила фильтрации в файле журнала и их расшифровка.

Значение	Описание
AC	*accept:* Принять пакет
DE	*delude:* В ответ на сообщение с установленным флагом SYN будет отправлено сообщение с флагами SYN-ACK, но в остальных случаях отправляется сообщение с флагом RST. Таким образом создается видимость того, что порт открыт и принимает подключения.
DR	*drop:* Отбросить пакет без уведомления
IN	*inspect:* Пересылка пакета, для которого было установлено соответствие системе предотвращения вторжений (IPS). Система предотвращения вторжений при этом должна быть включена. (При наличии сервиса idps)
RE	*reject:* Отбросить пакет и отправить сообщение ICMP с уведомлением хосту, пославшему пакет
TA	*tarpit:* При указании этого действия, в случае получения запроса на соединение, оно будет установлено, после чего размер окна будет установлен равным нулю, что вынудит систему, отправившую запрос на соединение, прекратить передачу данных. Любые попытки закрыть соединение игнорируются, таким образом соединение остается открытым, пока не истечет срок таймаута, что повлечет расходование локальных ресурсов системы, инициировавшей подключение, но не ресурсов Numa Edge (за исключением ресурсов системы отслеживания соединений, если она используется в МЭ).

Форма **set** этой команды используется для задания настройки регистрации событий фильтрации для указанного правила указанной политики.

Форма **delete** этой команды используется для удаления настройки регистрации событий фильтрации.

Форма **show** этой команды используется для отображения настройки регистрации событий фильтрации.

20.5.27 policy firewall <имя_политики> rule <номер_правила> match filter <фильтр>

Задание фильтра, который будет использоваться для выборки пакетов для указанного правила указанной политики.

Синтаксис

```
set policy firewall <имя_политики> rule <номер_правила> match filter <фильтр>
delete policy firewall <имя_политики> rule <номер_правила> match filter
show policy firewall <имя_политики> rule <номер_правила> match filter
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    firewall {
        имя_политики {
            rule номер_правила {
                match {
                    filter фильтр
                }
            }
        }
    }
}
```

Параметры

имя_политики

Имя политики межсетевого экранирования.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

фильтр

Пакетный фильтр, который будет использоваться указанным правилом данной политики межсетевого экранирования.

Значение по умолчанию

Не установлено.

Указания по использованию

Данная команда позволяет указать фильтр, который будет использоваться данным правилом указанной политики межсетевого экранирования. В правиле может быть указан только один фильтр, то есть новое указанное значение фильтра заменит предыдущее (при его наличии).

Форма **set** данной команды используется для указания фильтра, который будет использоваться данным правилом указанной политики межсетевого экранирования.

Форма **delete** данной команды позволяет удалить связь правила с каким-либо фильтром.

Форма **show** данной команды используется для отображения связанного с указанным правилом указанной политики межсетевого экранирования фильтра.

20.5.28 policy clear firewall <имя_политики>

Очистка статистики политики межсетевого экранирования IPv4-трафика.

Синтаксис

```
policy clear firewall <имя_политики>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики межсетевого экранирования IPv4-трафика.

Значение по умолчанию

Отсутствует.

20.5.29 policy clear firewall <имя_политики> rule <номер_правила>

Очистка статистики правила политики межсетевого экранирования IPv4-трафика.

Синтаксис

```
policy clear firewall <имя_политики> rule <номер_правила>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики межсетевого экранирования IPv4-трафика.

номер_правила

Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер.

Значение по умолчанию

Отсутствует.

20.5.30 policy clear firewall <имя_политики> rule <номер_правила> filter

Очистка статистики фильтра, связанного с указанным правилом политики межсетевого экранирования IPv4-трафика.

Синтаксис

```
policy clear firewall <имя_политики> rule <номер_правила> filter
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики межсетевого экранирования IPv4-трафика.

номер_правила

Численный идентификатор правила.

Значение по умолчанию

Отсутствует.

20.5.31 policy clear firewall <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>

Очистка статистики по указанному правилу фильтра, связанного с указанным правилом политики межсетевого экранирования IPv4-трафика.

Синтаксис

```
policy clear firewall <имя_политики> rule <номер_правила> filter rule
<номер_правила_фильтра>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики межсетевого экранирования IPv4-трафика.

номер_правила

Численный идентификатор правила.

номер_правила_фильтра

Численный идентификатор правила фильтра.

Значение по умолчанию

Отсутствует.

20.5.32 policy show firewall <имя_политики>

Вывод сведений и статистики для указанной политики межсетевого экранирования IPv4-трафика.

Синтаксис

```
policy show firewall <имя_политики>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики межсетевого экранирования IPv4-трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения сведений о выбранной настроенной политике межсетевого экранирования IPv4-трафика.

20.5.33 policy show firewall <имя_политики> rule <номер_правила>

Вывод конфигурации правила политики межсетевого экранирования IPv4-трафика.

Синтаксис

```
policy show firewall <имя_политики> rule <номер_правила>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики межсетевого экранирования IPv4-трафика.

номер_правила

Численный идентификатор правила.

Значение по умолчанию

Отсутствует.

20.5.34 policy show firewall <имя_политики> rule <номер_правила> filter

Вывод сведений и статистики по фильтру для указанного правила политики межсетевого экранирования IPv4.

Синтаксис

```
policy show firewall <имя_политики> rule <номер_правила> filter [detail | rule <номер_правила_фильтра>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики межсетевого экранирования IPv4-трафика.

номер_правила

Численный идентификатор правила.

detail

Вывод подробных сведений и статистики по фильтру для указанного правила политики межсетевого экранирования.

номер_правила фильтра

Вывод сведений и статистики по указанному правилу фильтра для указанного правила политики межсетевого экранирования.

Значение по умолчанию

Отсутствует.

20.5.35 named-list <тип_списка> export <имя_списка> to <имя_файла>

Экспорт именованных списков.

Синтаксис

```
named-list <тип_списка> export  <имя_списка> to <имя_файла>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

тип_списка

Тип экспортируемого именованного списка. Допустимые значения указаны в таблице ниже.

Таблица 165 – Типы именованных списков.

Значение	Описание
address	Именованный список адресов
domain	Именованный список доменов
port	Именованный список портов

имя_списка

Имя списка.

имя_файла

Путь до экспортируемого файла. Допустимые значения представлены в таблице ниже.

Таблица 166 – Способы экспорта именованных списков.

Местоположение	Способ указания
Путь в локальной системе	Может быть указан абсолютный или относительный путь в локальной системе. Используется стандартный способ указания файла в UNIX.
Сервер FTP	Используется следующий синтаксис для параметра *имя_файла*: ftp://*пользователь*@*узел*/*файл*

Местоположение	Способ указания
	где: *пользователь* – это имя пользователя на узле *узел* – это имя узла или IP-адрес сервера FTP *файл* – это название файла.
Сервер SCP	Используется следующий синтаксис для *имя_файла*: scp://*пользователь*@*узел*/*файл* где: *пользователь* – это имя пользователя на узле *узел* – это имя узла или IP-адрес сервера SCP *файл* – это название файла.
Сервер TFTP	Используется следующий синтаксис для параметра *имя_файла*: tftp://*узел*/*файл* где: *узел* – это имя узла или IP-адрес сервера TFTP *файл* – это название архива.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для экспорта именованных списков – списков адресов, доменных имен, подсетей или портов.

Производится экспорт именованного списка в файл по указанному адресу, который может быть локальным или находиться на сервере TFTP, FTP или SCP.

20.5.36 named-list <тип_списка> import <имя_списка> from <имя_файла>

Импорт именованных списков.

Синтаксис

```
named-list <тип_списка> import  <имя_списка> from <имя_файла>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

тип_списка

Тип экспортируемого именованного списка. Допустимые значения указаны в таблице ниже.

Таблица 167 – Типы именованных списков.

Значение	Описание
address	Именованный список адресов
domain	Именованный список доменов
port	Именованный список портов

имя_списка

Имя списка.

имя_файла

Путь до импортируемого файла. Допустимые значения представлены в таблице ниже.

Таблица 168 – Способы импорта именованных списков.

Местоположение	Способ указания
Путь в локальной системе	Может быть указан абсолютный или относительный путь в локальной системе. Используется стандартный способ указания файла в UNIX.
Сервер FTP	Используется следующий синтаксис для параметра *имя_файла*: ftp://*пользователь*@*узел*/*файл*

Местоположение	Способ указания
	где: *пользователь* – это имя пользователя на узле *узел* – это имя узла или IP-адрес сервера FTP *файл* – это название файла. Если *пользователь* не указан, будет выдан запрос на его ввод.
Сервер SCP	Используется следующий синтаксис для *имя_файла*: scp://*пользователь*@*узел*/*файл* где: *пользователь* – это имя пользователя на узле *узел* – это имя узла или IP-адрес сервера SCP *файл* – это название файла. Если *пользователь* и *пароль* не указаны, будет выдан запрос на их ввод.
Сервер TFTP	Используется следующий синтаксис для параметра *имя_файла*: tftp://*узел*/*файл* где: *узел* – это имя узла или IP-адрес сервера TFTP *файл* – это название файла.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для импорта именованных списков – списков адресов, доменных имен, подсетей или портов. Формат именованных списков: текстовый файл со значениями, разделенными между собой переносом строки.

При указании параметра from производится импорт из файла архива или текстового файла по указанному адресу, который может быть локальным или находиться на сервере TFTP, FTP или SCP.

20.5.37 named-list <тип_списка> remove <имя_списка>

Удаление именованного списка.

Синтаксис

```
named-list <тип_списка> remove <имя_списка>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

тип_списка

Тип экспортируемого именованного списка. Допустимые значения указаны в таблице ниже.

Таблица 169 – Типы именованных списков.

Значение	Описание
address	Именованный список адресов
domain	Именованный список доменов
port	Именованный список портов

имя_списка

Имя списка.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для удаления именнованного списка.

20.5.38 named-list <тип_списка> show

Отображение перечня именованных списков определенного типа, присутствующих в системе.

Синтаксис

```
named-list <тип_списка> show [<имя_списка>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

тип_списка

Тип экспортируемого именованного списка. Допустимые значения указаны в таблице ниже.

Таблица 170 – Типы именованных списков.

Значение	Описание
address	Именованный список адресов
domain	Именованный список доменов
port	Именованный список портов

имя_списка

Имя списка. При задании имени списка выводится содержимое конкретного списка.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения перечня именованных списков определенного типа, присутствующих в системе.

20.6 Команды межсетевого экрана IPv6

Команды настройки	
Команды для интерфейса	
interfaces <интерфейс> policy <направление> firewall-ipv6 <имя_политики>	Применение экземпляра межсетевого экрана IPv6 к определенному интерфейсу
Системные настройки	
system ipv6 receive-redirects <состояние>	Обработка сообщений IPv6 ICMP о перенаправлении.
system ipv6 source-route <состояние>	Обработка пакетов IPv6 с расширенным заголовком маршрутизации.
Правила и наборы правил (политики межсетевого экранирования)	
policy firewall-ipv6 <имя_политики>	Определение политики межсетевого экранирования IPv6.
policy firewall-ipv6 <имя_политики> default-action <действие>	Установка действия по умолчанию для политики межсетевого экранирования IPv6.
policy firewall-ipv6 <имя_политики> description <описание>	Указание краткого описания для политики межсетевого экранирования IPv6.
policy firewall-ipv6 <имя_политики> enable-default-log	Регистрация событий для действия по умолчанию указанной политики межсетевого экранирования
policy firewall-ipv6 <имя_политики> rule <номер_правила>	Определение правила в политике межсетевого экранирования IPv6.
policy firewall-ipv6 <имя_политики> rule <номер_правила> action <действие>	Указание действия, которое будет применяться к пакетам, для которых было установлено соответствие правилу.
policy firewall <имя_политики> rule <номер_правила> description <описание>	Указание краткого описания для правила в политике межсетевого экранирования IPv6.
policy firewall-ipv6 <имя_политики> rule <номер_правила> log <состояние>	Включение/выключение регистрации событий фильтрации трафика IPv6 для указанного правила указанной политики.

policy firewall-ipv6 <имя_политики> rule <номер_правила> match filter-ipv6 <фильтр>	Задание фильтра IPv6, который будет использоваться для выборки пакетов для указанного правила указанной политики IPv6.
Эксплуатационные команды	
policy clear firewall-ipv6 <имя_политики>	Очистка статистики для политики межсетевого экранирования IPv6.
policy clear firewall-ipv6 <имя_политики> rule <номер_правила>	Очистка статистики политики межсетевого экранирования IPv6-трафика.
policy clear firewall-ipv6 <имя_политики> rule <номер_правила> filter	Очистка статистики для фильтра, связанного с указанным правилом политики межсетевого экранирования IPv6-трафика.
policy clear firewall-ipv6 <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>	Очистка статистики по указанному правилу фильтра, связанного с указанным правилом политики межсетевого экранирования IPv6-трафика.
policy show firewall-ipv6 <имя_политики>	Вывод сведений и статистики для указанной политики межсетевого экранирования IPv6-трафика.
policy show firewall-ipv6 <имя_политики> rule <номер_правила>	Вывод сведений и статистики для указанного правила политики межсетевого экранирования IPv6-трафика.
policy show firewall-ipv6 <имя_политики> rule <номер_правила> filter	Вывод сведений и статистики по фильтру для указанного правила политики межсетевого экранирования IPv6.

20.6.1 interfaces <интерфейс> policy <направление> firewall-ipv6 <имя_политики>

Применение экземпляра межсетевого экрана IPv6 к определенному интерфейсу.

Синтаксис

```
set interfaces <интерфейс> policy <направление> firewall-ipv6 <имя_политики>

delete interfaces <интерфейс> policy <направление> firewall-ipv6 <имя_политики>

show interfaces <интерфейс> policy <направление> firewall-ipv6 <имя_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
    policy {
        направление {
            firewall-ipv6 имя_политики
        }
    }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже в разделе Указания по использованию.

направление

Обязательный. Направление трафика, к которому применяется политика межсетевого экранирования. Допустимые значения указаны в таблице ниже:

Таблица 171 – Направления трафика

Значение	Описание

in	Транзитный трафик IPv6, принимаемый на указанном интерфейсе
out	Транзитный трафик IPv6, отправляемый с указанного интерфейса
local	Трафик IPv6, принятый на интерфейсе, предназначенный для локальной системы.

имя_политики

Имя политики межсетевого экранирования.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет применить политику межсетевого экранирования IPv6 к интерфейсу.

Фильтрация транзитного трафика или трафика, предназначенного для локальной системы, не осуществляется до тех пор, пока политика межсетевого экранирования не будет применена к интерфейсу (реальному или виртуальному) с использованием данной команды.

Для включения межсетевого экранирования следует определить политику с помощью команды **policy firewall-ipv6**. Затем следует применить политику к интерфейсам и/или виртуальным интерфейсам, используя данную команду. После чего указанная политика межсетевого экранирования будет функционировать в качестве пакетного фильтра.

На каждом интерфейсе можно применить до трех политик межсетевого экранирования: одну как фильтр транзитного трафика, принимаемого на интерфейсе (in), одну – как фильтр транзитного трафика, покидающего интерфейс (out) и одну – как фильтр трафика, предназначенного для локальной системы (local).

В приведенной ниже таблице показаны типы поддерживаемых интерфейсов и синтаксис.

Таблица 172 – Типы интерфейсов

Тип интерфейса	**Синтаксис**
Агрегирование каналов	bonding bondx
Виртуальный интерфейс агрегированных каналов	bonding bondx vif идентификатор_vlan
Сетевой мост	bridge brx
Ethernet	ethernet ethx
Ethernet PPPoE	ethernet ethx pppoe номер
Виртуальный интерфейс Ethernet	ethernet ethx vif идентификатор_vlan
Ethernet Vif PPPoE	ethernet ethx vif идентификатор_vlan pppoe номер
Интерфейс заглушки	loopback lo
Многоканальная связь	multilink mlx
OpenVPN	openvpn vtunx
Псевдо-Ethernet	pseudo-ethernet pethx
Последовательный интерфейс	serial srx vif идентификатор_vlan
Туннель	tunnel tunx

Форма **set** данной команды позволяет применить политику межсетевого экранирования IPv6 к интерфейсу.

Форма **delete** данной команды позволяет удалить политику межсетевого экранирования IPv6 для интерфейса.

Форма **show** данной команды используется для отображения конфигурации политики межсетевого экранирования IPv6 на интерфейсе.

20.6.2 system ipv6 receive-redirects <состояние>

Обработка сообщений IPv6 ICMP о перенаправлении (тип 5).

Синтаксис

```
set system ipv6 receive-redirects <состояние>

delete system ipv6 receive-redirects

show system ipv6 receive-redirects
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system ipv6 {
   receive-redirects состояние
}
```

Параметры

состояние

Параметр обработки полученных пакетов перенаправлений IPv6 ICMP (тип 5). Допустимые значения:

enable: Система будет обрабатывать полученные пакетов перенаправлений IPv6 ICMP (тип 5);

disable: Система не будет обрабатывать полученные пакеты перенаправлений IPv6 ICMP (тип 5).

Значение по умолчанию

По умолчанию отправка пакетов перенаправлений IPv6 ICMP (тип 5) запрещена.

Указания по использованию

Данная команда позволяет разрешить или запретить отправку сообщений IPv6 ICMP о перенаправлении. Отправка сообщений redirect потенциально может изменить таблицу маршрутизации узла или маршрутизатора, которому предназначено сообщение.

Форма **set** данной команды позволяет разрешить или запретить отправку сообщений IPv6 ICMP о перенаправлении.

Форма **delete** данной команды позволяет удалить указанное значение.

Форма **show** позволяет отобразить указанное значение.

20.6.3 system ipv6 source-route <состояние>

Обработка пакетов IPv6 с расширенным заголовком маршрутизации.

Синтаксис

```
set system ipv6 source-route <состояние>
delete system ipv6 source-route
show system ipv6 source-route
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system ipv6 {
   source-route состояние
}
```

Параметры

состояние

Параметр обработки пакетов IPv6 с расширенным заголовком маршрутизации. Допустимые значения:

enable: Система будет обрабатывать пакеты IPv6 с расширенным заголовком маршрутизации;

disable: Система не будет обрабатывать пакеты IPv6 с расширенным заголовком маршрутизации.

Значение по умолчанию

По умолчанию пакеты IPv6 с расширенным заголовком маршрутизации не обрабатываются.

Указания по использованию

Маршрутизация от источника разрешает приложениям указать один или несколько промежуточных адресов получателя для исходящих пакетов в обход таблицы маршрутизации. Данная возможность в некоторых случаях используется для выявления неисправностей, но делает сеть уязвимой к атакам, при которых сетевой трафик перенаправляется через централизованную точку записи трафика.

Данная команда позволяет разрешить или запретить обработку пакетов IPv6 с расширенным заголовком маршрутизации.

Форма **set** данной команды позволяет разрешить или запретить обработку пакетов IPv6 с расширенным заголовком маршрутизации.

Форма **delete** данной команды позволяет удалить указанное значение.

Форма **show** позволяет отобразить указанное значение.

20.6.4 policy firewall-ipv6 <имя_политики>

Определение набора правил IPv6 межсетевого экрана.

Синтаксис

```
set policy firewall-ipv6 <имя_политики>
delete policy firewall-ipv6 [<имя_политики>]
show policy firewall-ipv6 [<имя_политики>]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   firewall-ipv6 {
      имя_политики {
      }
   }
}
```

Параметры

имя_политики

Множественный узел. Текст. Имя политики межсетевого экранирования. Можно определить несколько политик межсетевого экранирования IPv6, создав соответствующее количество узлов конфигурации.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет определить политику межсетевого экранирования IPv6. Политика межсетевого экранирования может включать в себя до 65 535 правил.

Форма **set** данной команды используется для создания и изменения политики межсетевого экранирования IPv6.

Форма **delete** данной команды используется для удаления политики межсетевого экранирования IPv6.

Форма **show** данной команды используется для отображения настройки политики межсетевого экранирования IPv6.

20.6.5 policy firewall-ipv6 <имя_политики> default-action <действие>

Установка действия по умолчанию для набора правил IPv6.

Синтаксис

```
set policy firewall-ipv6 <имя_политики> default-action <действие>
```

```
delete policy firewall-ipv6 <имя_политики> default-action
show policy firewall-ipv6 <имя_политики> default-action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   firewall-ipv6 {
      имя_политики {
         default-action действие
      }
   }
}
```

Параметры

имя_политики

Имя политики межсетевого экранирования.

действие

Действие по умолчанию, которое осуществляется в том случае, если для политики не было установлено ни одного соответствия. Допустимые значения представлены в таблице ниже.

Таблица 173 – Действия по умолчанию для политик межсетевого экранирования.

Значение	Описание
accept	Принять пакет
drop	Отбросить пакет без уведомления
reject	Отбросить пакет и отправить сообщение ICMP с уведомлением хосту, пославшему пакет

Значение по умолчанию

В том случае если действие по умолчанию явно не указано, в том случае если для пакета не было установлено ни одного соответствия в наборе правил, пакет отбрасывается без уведомления.

Указания по использованию

Данная команда позволяет указать действие по умолчанию, которое будет выполняться в том случае, если для пакета не было установлено ни одного соответствия правилам политики межсетевого экранирования IPv6.

В том случае если для пакета не было установлено соответствие ни одному правилу в наборе, к нему применяется политика, принятая по умолчанию. По умолчанию, пакет отбрасывается без отправки сообщения ICMP с уведомлением о том, что адресат недоступен .

Форма **set** данной команды позволяет установить действие по умолчанию для набора правил IPv6.

Форма **delete** данной команды используется для восстановления поведения по умолчанию для пакетов, для которых не было установлено ни одного соответствия критериям правила.

Форма **show** данной команды используется для отображения настройки политики по умолчанию.

20.6.6 policy firewall-ipv6 <имя_политики> description <описание>

Указание краткого описания для политики межсетевого экранирования IPv6.

Синтаксис

```
set policy firewall-ipv6 <имя_политики> description <описание>
delete policy firewall-ipv6 <имя_политики> description
show policy firewall-ipv6 <имя_политики> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    firewall-ipv6 {
        имя_политики {
            description описание
        }
    }
}
```

Параметры

имя_политики

Имя политики межсетевого экранирования.

описание

Описание политики межсетевого экранирования. В том случае если описание содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать описание для политики межсетевого экранирования IPv6.

Форма **set** данной команды используется для создания и изменения описания.

Форма **delete** используется для удаления описания.

Форма **show** используется для отображения настройки описания.

20.6.7 policy firewall-ipv6 <имя_политики> enable-default-log

Регистрация событий для действия по умолчанию указанной политики межсетевого экранирования

Синтаксис

```
set policy firewall-ipv6 <имя_политики> enable-default-log
delete policy firewall-ipv6 <имя_политики> enable-default-log
show policy firewall-ipv6 <имя_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    firewall-ipv6 {
        имя_политики {
            enable-default-log
        }
    }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет включить регистрацию событий для действия по умолчанию указанной политики межсетевого экранирования IPv6.

Форма **set** данной команды используется для включения регистрации событий для действия по умолчанию указанной политики межсетевого экранирования IPv6.

Форма **delete** используется для отключения регистрации событий для действия по умолчанию указанной политики межсетевого экранирования IPv6.

Форма **show** используется для отображения настройки.

20.6.8 policy firewall-ipv6 <имя_политики> rule <номер_правила>

Определение правила в наборе правил межсетевого экрана IPv6.

Синтаксис

```
set policy firewall-ipv6 <имя_политики> rule <номер_правила>
delete policy firewall-ipv6 <имя_политики> rule [<номер_правила>]
show policy firewall-ipv6 <имя_политики> rule [<номер_правила>]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    firewall-ipv6 {
        имя_политики {
            rule номер_правила {
            }
        }
    }
}
```

Параметры

имя_политики

Имя политики межсетевого экранирования.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65 535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет определить правило в политике межсетевого экранирования IPv6. Политика может включать в себя до 65 535 настраиваемых правил.

Правила политики исполняются в порядке следования их номеров, от наименьшего к наибольшему. Напрямую изменить номер правила нельзя, так как он является идентификатором узла конфигурации; однако, можно изменять номера правил при помощи команды **rename**.

Для того чтобы не прибегать к изменению номеров правил, хорошей практикой является указание номеров с шагом 10. Это позволяет оставить пространство, куда можно будет впоследствии добавить новые правила.

Форма **set** данной команды используется для создания или изменения правила в политике межсетевого экранирования IPv6.

Форма **delete** данной команды используется для удаления правила из политики межсетевого экранирования IPv6.

Форма **show** данной команды используется для отображения настройки правила политики межсетевого экранирования IPv6.

20.6.9 policy firewall-ipv6 <имя_политики> rule <номер_правила> action <действие>

Указание действия, которое будет применяться к пакетам, для которых было установлено соответствие правилу.

Синтаксис

```
set policy firewall-ipv6 <имя_политики> rule <номер_правила> action <действие>
delete policy firewall-ipv6 <имя_политики> rule <номер_правила> action
show policy firewall-ipv6 <имя_политики> rule <номер_правила> action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    firewall-ipv6 {
        имя_политики {
            rule номер_правила {
                action действие
            }
        }
    }
}
```

Параметры

имя_политики

Имя политики межсетевого экранирования.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65 535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

действие

Действие, которое будет выполнено, в том случае если пакет удовлетворяет критериям, указанным в правиле. Допустимые значения представлены в таблице ниже.

Таблица 174 – Действия для правил политик межсетевого экранирования.

Значение	Описание
accept	Принять пакет
drop	Отбросить пакет без уведомления

inspect	Пересылка пакета, для которого было установлено соответствие системе предотвращения вторжений (IPS). Система предотвращения вторжений при этом должна быть включена. (При наличии сервиса idps)
reject	Отбросить пакет и отправить сообщение ICMP с уведомлением хосту, пославшему пакет

Значение по умолчанию

Пакеты отбрасываются.

Указания по использованию

Данная команда позволяет указать действие, которое будет применено к пакетам, для которых было установлено соответствие критериям, указанным в правиле. В правиле может быть указано только одно действие.

Форма **set** данной команды используется для указания действия, которое будет применяться к пакетам, для которых установлено соответствие критериям правила.

Форма **delete** данной команды позволяет восстановить действие, принятое по умолчанию.

Форма **show** данной команды используется для отображения настройки действия для правила политики межсетевого экранирования IPv6.

20.6.10 policy firewall <имя_политики> rule <номер_правила> description <описание>

Указание краткого описания для политики межсетевого экранирования IPv6.

Синтаксис

```
set policy firewall <имя_политики> rule <номер_правила> description <описание>

delete policy firewall <имя_политики> rule <номер_правила> description

show policy firewall <имя_политики> rule <номер_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    firewall {
        имя_политики {
            rule номер_правила {
                description описание
            }
        }
    }
}
```

Параметры

имя_политики

Имя политики межсетевого экранирования.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65 535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

описание

Описание правила в политике межсетевого экранирования. В том случае если описание содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать описание правила в политике межсетевого экранирования.

Форма **set** данной команды используется для создания и изменения описания.

Форма **delete** используется для удаления описания.

Форма **show** используется для отображения настройки описания.

20.6.11 policy firewall-ipv6 <имя_политики> rule <номер_правила> log <состояние>

Включение/выключение регистрации событий фильтрации трафика IPv6 для указанного правила указанной политики.

Синтаксис

```
set policy firewall-ipv6 <имя_политики> rule <номер_правила> log <состояние>
delete policy firewall-ipv6 <имя_политики> rule <номер_правила> log
show policy firewall-ipv6 <имя_политики> rule <номер_правила> log
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   firewall-ipv6 {
      имя_политики {
         rule номер_правила {
            log состояние
         }
      }
   }
}
```

Параметры

имя_политики

Имя определённой политики фильтрации трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

состояние

Указывает режим регистрации событий для правил политики. Допустимые значения:

enable: Включение регистрации событий фильтрации для правила политики;

disable: Отключение регистрации событий фильтрации для правила политики.

Значение по умолчанию

Отсутствует.

Указания по использованию

Включает или отключает журналирование событий для правила политики.

В том случае, если задействовано журналирование для правила политики, в системный лог (журнал) будут выводиться сообщения для всех пакетов IPv6, подпадающих под правило.

Для каждого сообщения формируется префикс в квадратных скобках вида **[f6-<имя_политики>-<номер правила>-<действие>]**

Имя политики может быть записано в журнале не полностью в связи с системным ограничением общей длины префикса в 29 символов. Действия в файле журнала кодируются следующими аббревиатурами:

Таблица 175 – Аббревиатуры действий правила фильтрации в файле журнала и их расшифровка.

Значение	Описание
AC	*accept:* Принять пакет
DR	*drop:* Отбросить пакет без уведомления
IN	*inspect:* Пересылка пакета, для которого было установлено соответствие системе предотвращения вторжений (IPS). Система предотвращения вторжений при этом должна быть включена. (При наличии сервиса idps)
RE	*reject:* Отбросить пакет и отправить сообщение ICMP с уведомлением хосту, пославшему пакет

Форма **set** этой команды используется для задания настройки регистрации событий фильтрации для указанного правила указанной политики IPv6.

Форма **delete** этой команды используется для удаления настройки регистрации событий фильтрации.

Форма **show** этой команды используется для отображения настройки регистрации событий фильтрации.

20.6.12 policy firewall-ipv6 <имя_политики> rule <номер_правила> match filter-ipv6 <фильтр>

Задание фильтра, который будет использоваться для выборки пакетов для указанного правила указанной политики IPv6.

Синтаксис

```
set policy firewall-ipv6 <имя_политики> rule <номер_правила> match filter-ipv6 <фильтр>

delete policy firewall-ipv6 <имя_политики> rule <номер_правила> match filter-ipv6

show policy firewall-ipv6 <имя_политики> rule <номер_правила> match filter-ipv6
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    firewall-ipv6 {
        имя_политики {
            rule номер_правила {
                match {
                    filter-ipv6 фильтр
                }
            }
        }
    }
}
```

Параметры

имя_политики

Имя политики межсетевого экранирования.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

фильтр

Пакетный фильтр, который будет использоваться указанным правилом данной политики межсетевого экранирования IPv6.

Значение по умолчанию

Не установлено.

Указания по использованию

Данная команда позволяет указать фильтр, который будет использоваться данным правилом указанной политики межсетевого экранирования IPv6. В правиле может быть указан только один фильтр, то есть новое указанное значение фильтра заменит предыдущее (при его наличии).

Форма **set** данной команды используется для указания фильтра, который будет использоваться данным правилом указанной политики межсетевого экранирования IPv6.

Форма **delete** данной команды позволяет удалить связь правила с каким-либо фильтром.

Форма **show** данной команды используется для отображения связанного с указанным правилом указанной политики межсетевого экранирования фильтра.

20.6.13 policy clear firewall-ipv6 <имя_политики>

Очистка статистики политики межсетевого экранирования IPv6-трафика.

Синтаксис

```
policy clear firewall-ipv6 <имя_политики>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики межсетевого экранирования IPv6-трафика.

Значение по умолчанию

Отсутствует.

20.6.14 policy clear firewall-ipv6 <имя_политики> rule <номер_правила>

Очистка статистики правила политики межсетевого экранирования IPv6-трафика.

Синтаксис

```
policy clear firewall-ipv6 <имя_политики> rule <номер_правила>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики межсетевого экранирования IPv6-трафика.

номер_правила

Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер.

Значение по умолчанию

Отсутствует.

20.6.15 policy clear firewall-ipv6 <имя_политики> rule <номер_правила> filter

Очистка статистики для фильтра, связанного с указанным правилом политики межсетевого экранирования IPv6-трафика.

Синтаксис

```
policy clear firewall-ipv6 <имя_политики> rule <номер_правила> filter
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики межсетевого экранирования IPv6-трафика.

номер_правила

Численный идентификатор правила.

Значение по умолчанию

Отсутствует.

20.6.16 policy clear firewall-ipv6 <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>

Очистка статистики по указанному правилу фильтра, связанного с указанным правилом политики межсетевого экранирования IPv6-трафика.

Синтаксис

```
policy clear firewall-ipv6 <имя_политики> rule <номер_правила> filter rule
<номер_правила_фильтра>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики межсетевого экранирования IPv6-трафика.

номер_правила

Численный идентификатор правила.

номер_правила_фильтра

Численный идентификатор правила фильтра.

Значение по умолчанию

Отсутствует.

20.6.17 policy show firewall-ipv6 <имя_политики>

Вывод сведений и статистики для указанной политики межсетевого экранирования IPv6-трафика.

Синтаксис

```
policy show firewall <имя_политики>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики межсетевого экранирования IPv6-трафика.

Указания по использованию

Эта команда используется для отображения сведений о выбранной настроенной политике межсетевого экранирования IPv6-трафика.

20.6.18 policy show firewall-ipv6 <имя_политики> rule <номер_правила>

Вывод конфигурации правила политики межсетевого экранирования IPv6-трафика.

Синтаксис

```
policy show firewall-ipv6 <имя_политики> rule <номер_правила>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики межсетевого экранирования IPv6-трафика.

номер_правила

Численный идентификатор правила.

Значение по умолчанию

Отсутствует.

20.6.19 policy show firewall-ipv6 <имя_политики> rule <номер_правила> filter

Вывод сведений и статистики по фильтру для указанного правила политики межсетевого экранирования IPv6.

Синтаксис

```
policy show firewall <имя_политики> rule <номер_правила> filter [detail |
rule <номер_правила_фильтра>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики межсетевого экранирования IPv6-трафика.

номер_правила

Численный идентификатор правила.

detail

Вывод подробных сведений и статистики по фильтру для указанного правила политики межсетевого экранирования IPv6.

r*ule номер_правила фильтра*

Вывод сведений и статистики по указанному правилу фильтра для указанного правила политики межсетевого экранированияIPv6.

Значение по умолчанию

Отсутствует.

21 Межсетевой экран на основе зон

21.1 Описание

Обычные политики межсетевого экранирования применяются к каждому интерфейсу в отдельности и позволяют осуществлять фильтрацию для различных направлений трафика (входящий, исходящий и локальный) для каждого интерфейса. Данный метод организации межсетевого экрана удобен для небольших сетевых топологий. Однако по мере усложнения сетевой инфраструктуры, добавления различных виртуальных интерфейсов (VLAN, openvpn и т.д) и при необходимости детального контроля входящего и исходящего трафика на различных интерфейсах, результирующая конфигурация существенно увеличивается. Межсетевой экран на основе зон обладает рядом особенностей, которые позволяют элегантнее организовывать защиту периметра организации.

Основной абстракцией для данной организации межсетевого экрана являются зоны. Правила межсетевого экранирования применяются для трафика, который передается из одной зоны в другую. Существуют два типа зон:

- Транзитная зона — зона, объединяющая один или несколько сетевых интерфейсов, где адресом назначения трафика является какое-либо внешнее устройство.
- Локальная зона — зона, обозначающая сам межсетевой экран и все его интерфейсы. Используется для трафика, адресом назначения которого является сам межсетевой экран.

ПРИМЕЧАНИЕ: Система конфигурации позволяет создать транзитную зону, в которой отсутствуют интерфейсы. Данная особенность удобна для первоначальной настройки, но необходимо иметь в виду, что транзитная зона без интерфейсов не имеет практического смысла, так как трафик не поступает в данную зону.

Основным отличием данных типов зон является то, что для транзитной зоны по умолчанию запрещен весь входящий и исходящий трафик, в то время как для локальной зоны — разрешен. Таким образом, для транзитных зон правила межсетевого экранирования должны описывать разрешаемый тип трафика, и для локальной зоны, наоборот, запрещаемый.

Другие особенности реализации межсетевого экрана на основе зон:

- В пределах зоны между различными интерфейсами разрешен весь трафик.
- Каждый интерфейс может быть связан только с одной транзитной зоной.
- К интерфейсу, принадлежащему к транзитной зоне, не может быть применена индивидуальная для этого интерфейса политика межсетевого экранирования, и наоборот.
- Трафик между интерфейсами, не принадлежащими к транзитным зонам, передается без фильтрации, и к этим интерфейсам могут быть применены индивидуальные политики межсетевого экранирования.

ПРИМЕЧАНИЕ: Управляющий интерфейс (ethm) не относится ни к одной из зон и средствами системы конфигурации его так же нельзя добавить в транзитную зону. Поэтому возможен обмен трафиком между управляющим интерфейсом и локальной зоной, а так же между ним и другими интерфейсами, не принадлежащими к транзитным зонам.

21.2 Примеры настройки межсетевого экрана на основе зон

В этом примере производится довольно типичное разделение инфраструктуры компании на три зоны безопасности:

- зона WAN — в данную зону добавляется uplink. Разрешена инициализация соединений с определенными сервисами в зоне DMZ и запрещена инициализация всех соединений с зоной LAN;
- зона LAN — в данную зону добавляются интерфейсы внутренней сети компании. Разрешена установка соединений с зоной WAN и зоной DMZ.
- зона DMZ — в данную зону выносятся сервисы, к которым необходимо осуществлять доступ из зоны WAN. Запрещены исходящие соединения в зону LAN.

На рисунке 45 показан пример реализации данной концепции:

- Имеются три транзитных зоны (то есть точки, где трафик проходит через маршрутизатор): закрытая зона, демилитаризованная зона (DMZ) и общедоступная зона.
- Интерфейс **eth1** лежит в общедоступной зоне; **eth2** лежит в DMZ; **eth3** и **eth4** лежат в закрытой зоне.
- Стрелки из одной зоны в другую представляют политики фильтрации трафика, применяемые к трафику, передаваемому между зонами.
- Трафик, передаваемый между 10.10.3.0/24 и 10.10.4.0/24, остаётся в одной и той же зоне безопасности, так что трафик между этими подсетями передается без фильтрации.

Помимо трех транзитных зон, на рисунке 45 есть и четвёртая зона – локальная зона, описывающая сам межсетевой экран.

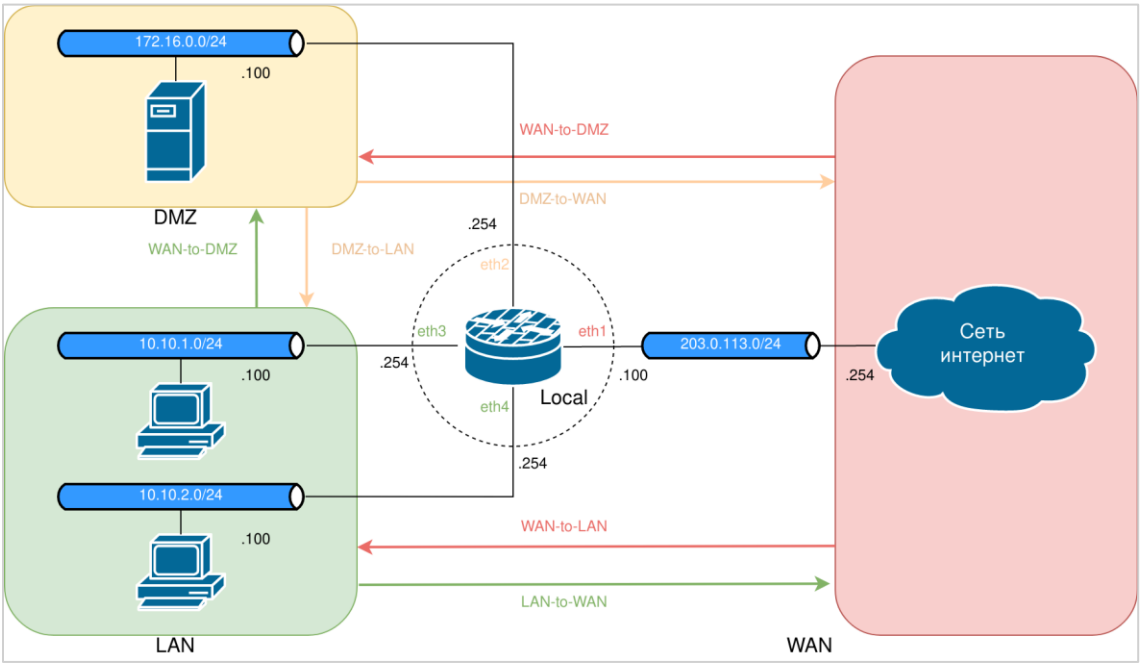


Рисунок 45 - Межсетевой экран, основанный на политиках зон безопасности

21.2.1 Начальная настройка IP-адресации

На рисунке 45 приведена схема сетевой адресации внутри организации. Для удобства данная схема представлена в виде таблицы 176.

Таблица 176 – IP-адресация внутри организации

Подсеть	IP адрес	Устройство	Зона
203.0.113.0/24	203.0.113.100	Numa Edge#eth1	WAN
	203.0.113.254	Шлюз провайдера	WAN
172.16.0.0/24	172.16.0.100	Сервер организации	DMZ
	172.16.0.254	Numa Edge#eth2	DMZ
10.10.1.0/24	10.10.1.100	APM1	LAN
	10.10.1.254	Numa Edge#eth3	LAN
10.10.2.0/24	10.10.2.100	APM2	LAN
	10.10.2.254	Numa Edge#eth4	LAN

Для настройки данных подсетей в Numa Edge перейдите в конфигурационный режим и выполните следующие команды:

Пример 185 – Отображение узла конфигурации "show policy firewall"

Действие	Команда
Настройка внешнего IP адреса из подсети провайдера на интерфейсе eth1.	`[edit]` `admin@edge# set interfaces ethernet eth1 address 203.0.113.100/24`
Задание описания к данному интерфейсу.	`[edit]`

Действие	Команда
	admin@edge# set interfaces ethernet eth1 description Uplink
Задание IP адреса на интерфейсе, к которому подключаются сервера организации.	[edit] admin@edge# set interfaces ethernet eth2 address 172.16.0.254/24
Установка описания для этого интерфейса.	[edit] admin@edge# set interfaces ethernet eth2 description DMZ
Настройка IP адреса на одном из интерфейсов, к которому подключаются рабочие ПК в организации.	[edit] admin@edge# set interfaces ethernet eth3 address 10.10.1.254/24
Добавление описания.	[edit] admin@edge# set interfaces ethernet eth3 description LAN1
Настройка IP адреса на втором интерфейсе для рабочих ПК.	[edit] admin@edge# set interfaces ethernet eth4 address 10.10.2.254/24
Добавления описания.	[edit] admin@edge# set interfaces ethernet eth4 description LAN2
Применение изменений	[edit] admin@edge# commit

Просмотр получившейся конфигурации ethernet интерфейсов.	[edit]
	admin@edge# show interfaces ethernet
	eth1 {
	address 203.0.113.100/24
	description Uplink
	}
	eth2 {
	address 172.16.0.254/24
	description DMZ
	}
	eth3 {
	address 10.10.1.254/24
	description LAN1
	}
	eth4 {
	address 10.10.2.254/24
	description LAN2
	}

Настройка других сетевых устройств в данном примере не рассматривается.

Проверка сетевой связности между устройствами

После настройки сетевой связности рекомендуется произвести проверку доступности устройств между собой. В дальнейшем проверка работы правил фильтрации сетевого трафика будет заключаться именно в проверке доступности или недоступности устройств, расположенных в различных зонах. Начальная и конечная проверки будут включать в себя генерацию ICMP трафика в следующих направлениях:

- Из LAN в LAN — передача трафика внутри одной зоны.
- Из LAN в WAN — доступ в интернет для локальных пользователей.
- Из WAN в LAN — проверка возможности установки соединения из интернета в локальную сеть (должно быть запрещено).
- Из WAN в DMZ — проверка доступности внутренних сервисов из интернета.
- Из DMZ в EDGE — доступ из сервисной сети за сам маршрутизатор должен быть запрещен.
- Из LAN в EDGE — проверка возможности управления устройством из локальной сети.
- Из LAN в DMZ — проверка доступности внутренних сервисов внутри сети.

Данный набор тестов выбран на основании того, что затрагивает различные политики фильтрации трафика, но в то же время не является слишком избыточным. Например, для трафика между зонами LAN и WAN

будет применен точно такой же набор политик, что и между зонами EDGE и WAN, поэтому имеет смысл проверять только один из этих наборов. Подробности взаимодействия политик фильтрации между зонами описаны далее в документе. Используется IP адресация устройств согласно таблице 1.

В данной проверке ожидается, что все устройства будут доступны по сети.

Тест 1, результат – OK.

Из LAN в LAN , scr ip = 10.10.1.100, dst ip = 10.10.2.100

```
root@LAN1:~# ping 10.10.2.100 -c 1
PING 10.10.2.100 (10.10.2.100) 56(84) bytes of data.
64 bytes from 10.10.2.100: icmp_seq=1 ttl=63 time=1.50 ms

--- 10.10.2.100 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.502/1.502/1.502/0.000 ms
root@LAN1:~#
```

Тест 2, результат – OK.

Из LAN в WAN, src ip = 10.10.1.100, dst ip = 203.0.113.254

```
root@LAN1:~# ping 203.0.113.254  -c 1
PING 203.0.113.254 (203.0.113.254) 56(84) bytes of data.
64 bytes from 203.0.113.254: icmp_seq=1 ttl=63 time=1.37 ms

--- 203.0.113.254 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.373/1.373/1.373/0.000 ms
root@LAN1:~#
```

ПРИМЕЧАНИЕ: В реальном применении для доступа устройств из локальной сети в сеть интернет потребуется настройка NAT для сокрытия адресного пространства локальной сети. Настройка NAT не рассматривается в данном примере.

Тест 3, результат – OK.

Из WAN в LAN, src ip = 203.0.113.1 dst ip = 10.10.2.100

```
root@WAN:~# ping 10.10.2.100 -c 1
PING 10.10.2.100 (10.10.2.100) 56(84) bytes of data.
64 bytes from 10.10.2.100: icmp_seq=1 ttl=63 time=1.46 ms

--- 10.10.2.100 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.462/1.462/1.462/0.000 ms
```

Тест 4, результат – OK.

Из WAN в DMZ, src ip = 203.0.113.254 dst ip = 172.16.0.100

```
root@WAN:~# ping 172.16.0.100 -c 1
PING 172.16.0.100 (172.16.0.100) 56(84) bytes of data.
64 bytes from 172.16.0.100: icmp_seq=1 ttl=63 time=1.47 ms

--- 172.16.0.100 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.466/1.466/1.466/0.000 ms
```

Тест 5, результат – OK.

Из DMZ в EDGE, src ip = 172.16.0.100 dst ip = 172.16.0.254

```
root@DMZ:~# ping 10.10.1.254 -c 1
PING 172.16.0.254 (172.16.0.254) 56(84) bytes of data.
64 bytes from 172.16.0.254: icmp_seq=1 ttl=64 time=0.797 ms

--- 172.16.0.254 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.797/0.797/0.797/0.000 ms
```

ПРИМЕЧАНИЕ: В данном тесте для проверки в качестве адреса получателя используется IP адрес 172.16.0.100 настроенный на интерфейсе eth2, который принадлежит к зоне LAN. Необходимо помнить что если адресом назначения трафика является любой IP адрес, настроенный на Numa Edge, то в не зависимости от принадлежности интерфейса к транзитной зоне, данный трафик относится к локальной зоне (в данном случае – EDGE).

Тест 6, результат – OK.

Из LAN в EDGE, src ip = 10.10.1.100 dst ip = 10.10.1.254

```
root@LAN1:~# ping 10.10.1.254 -c 1
PING 10.10.1.254 (10.10.1.254) 56(84) bytes of data.
64 bytes from 10.10.1.254: icmp_seq=1 ttl=64 time=0.720 ms

--- 10.10.1.254 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.720/0.720/0.720/0.000 ms
```

Тест 7, результат – OK.

Из LAN в DMZ, src ip = 10.10.1.100 dst ip = 172.16.1.100

```
root@LAN1:~# ping 172.16.0.100 -c 1
PING 172.16.0.100 (172.16.0.100) 56(84) bytes of data.
64 bytes from 172.16.0.100: icmp_seq=1 ttl=63 time=1.40 ms

--- 172.16.0.100 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.404/1.404/1.404/0.000 ms
```

21.2.2 Создание зон безопасности

Создание транзитных зон и добавление в них сетевых интерфейсов

Первоначально производится создание транзитных зон и добавление в них сетевых интерфейсов согласно таблице 176. Для этого выполните следующие действия:

Пример 186 – Отображение узла конфигурации "show policy firewall"

Действие	Команда
Создание узла конфигурации для зоны WAN и добавление описания к ней.	[edit] admin@edge# set zone-policy zone WAN description "WAN ZONE"
Добавление интерфейса eth1 к этой зоне.	[edit] admin@edge# set zone-policy zone WAN interface eth1
Создание узла конфигурации для зоны DMZ и добавление описания к ней.	[edit] admin@edge# set zone-policy zone DMZ description "DMZ ZONE"
Добавление интерфейса eth2 к зоне DMZ.	[edit] admin@edge# set zone-policy zone DMZ interface eth2
Создание узла конфигурации для зоны LAN и добавление описания к ней.	[edit] admin@edge# set zone-policy zone LAN

Действие	Команда
	`description "LAN ZONE"`
Добавление интерфейса eth3 к зоне.	`[edit]` `admin@edge# set zone-policy zone LAN interface eth3`
Добавление интерфейса eth4 к зоне.	`[edit]` `admin@edge# set zone-policy zone LAN interface eth4`
Применение изменений.	`[edit]` `admin@edge# commit`

Вывод конфигурации узла zone-policy.	`[edit]`
	`admin@edge# show zone-policy`
	`zone DMZ {`
	`description "DMZ ZONE"`
	`interface eth2`
	`}`
	`zone LAN {`
	`description "LAN ZONE"`
	`interface eth3`
	`interface eth4`
	`}`
	`zone WAN {`
	`description "WAN ZONE"`
	`interface eth1`
	`}`

Обратите внимание, что после применения данной конфигурации, передача трафика между транзитными зонами будет запрещена. Это связано с тем, что для каждой транзитной зоны по умолчанию (если пакет не попадает ни под одну из политик) используется действие **drop**. Система конфигурации позволяет изменить данное действие на значения:

- reject — запрет трафика с уведомлением отправителя;
- accept — разрешение трафика.

Изменение значения для данного атрибута осуществляется с помощью команды:

```
admin@edge# set zone-policy zone <zone-name> default-action
Possible completions:
  accept        Пропустить
  drop          Удалить без нотификации
  reject        Удалить и послать сообщение источнику
```

ВАЖНО: Изменять данные значения не рекомендуется, поскольку они влияют на весь входящий и исходящий трафик, не попадающий под другие политики. Изменения этих значений для транзитных зон может существенно подорвать их безопасность.

Дополнительно следует заметить, что поскольку интерфейсы eth1 и eth2 лежат в одной и той же зоне, передача трафика между ними происходит беспрепятственно.

Создание локальной зоны

Для создания локальной зоны необходимо выполнить следующие команды:

Пример 187 – Создание локальной зоны

Действие	Команда
Создание локальной зоны.	`[edit]` `admin@edge# set zone-policy zone EDGE local-zone`
Добавление описания.	`[edit]` `admin@edge# set zone-policy zone EDGE description "Numa Edge local zone"`
Применение конфигурации	`[edit]` `admin@edge# commit`

Действие	Команда

Просмотр всех настроенных зон на устройстве	[edit]
	admin@edge# show zone-policy
	zone DMZ {
	description "DMZ ZONE"
	interface eth2
	}
	zone EDGE {
	description "Numa Edge local zone"
	local-zone
	}
	zone LAN {
	description "LAN ZONE"
	interface eth3
	interface eth4
	}
	zone WAN {
	description "WAN ZONE"
	interface eth1
	}

Теперь межсетевой экран разделен на зоны безопасности и необходимо настроить политики фильтрации трафика между этими зонами.

21.2.3 Настройка политик фильтрации трафика между зонами

Настройка базовых политик фильтрации

Перед началом настройки сложных правил фильтрации, которые описывают различные условия прохождения трафика будет полезно создать простые правила, явно запрещающие или разрешающие приходящий трафик в определенную зону.

Для этого необходимо настроить следующие политики:

- "ALL_ACCEPT" — безусловно разрешающая политика для передачи трафика между транзитными зонами.
- "ALLOW_RESPONSE" — политика на основе состояния соединения, разрешающая только ответный трафик;
- "ALL_DROP" — безусловная запрещающая политика для передачи трафика между транзитными зонами и локальной зоной;

Данные политики являются довольно универсальными, и в дальнейшем могут применяться для разрешения трафика между различными зонами в случае увеличения их количества.

Пример 188 – Создание безусловно разрешающей политики

Действие	Команда
Создание узла конфигурации для политики ALL_ACCEPT и ввод описания для неё.	[edit] admin@edge# set policy firewall ALL_ACCEPT description "allow all traffic"
Создание правила для принятия всего трафика, передаваемого в общедоступную зону.	[edit] admin@edge# set policy firewall ALL_ACCEPT default-action accept
Фиксация настройки.	[edit] admin@edge# commit
Вывод настройки межсетевого экрана.	[edit] admin@edge# show policy firewall ALL_ACCEPT default-action accept description "allow all traffic"

Теперь создается политика, которая разрешает только ответный трафик.

Пример 189 – Создание политики разрешающий ответный трафик

Действие	Команда
Создание правила фильтрации для разрешения прохождения только трафика, исходящего из	[edit] admin@edge# set filter STATE-GOOD rule 10

этой зоны (т.е. ранее установленные сеансы и связанный с ними трафик).	state established enable [edit] admin@edge# set filter STATE-GOOD rule 10 state related enable [edit] admin@edge# set filter STATE-GOOD rule 10 protocol all
Создание узла конфигурации для политики ALLOW_RESPONSE и ввод описания для неё.	[edit] admin@edge# set policy firewall ALLOW_RESPONSE description "filter traffic to LAN zone"
Создание правила rule 10 для политики межсетевого экранирования ALLOW_RESPONSE. Это правило разрешает трафик, соответствующий указанным критериям.	[edit] admin@edge# set policy firewall ALLOW_RESPONSE rule 10 action accept
Применение фильтра STATE-GOOD к политике межсетевого экрана ALLOW_RESPONSE.	[edit] admin@edge# set policy firewall ALLOW_RESPONSE rule 10 match filter STATE-GOOD
Фиксация настройки.	[edit] admin@edge# commit

Вывод настройки межсетевого экрана.	[edit]
	admin@edge# show filter STATE-GOOD
	rule 10 {
	protocol all
	state {
	established enable
	related enable
	}
	}
	[edit]
	admin@edge# show policy firewall ALLOW_RESPONSE
	description "filter traffic to LAN zone"
	rule 10 {
	action accept
	match {
	filter STATE-GOOD
	}
	}

Далее создается безусловно запрещающая политика.

Пример 190 – Создание безусловно разрешающей политики

Действие	**Команда**
Создание узла конфигурации для политики ALL_ACCEPT и ввод описания для неё.	[edit] admin@edge# set policy firewall ALL_DROP description "drop all traffic"
Создание правила для принятия всего трафика, передаваемого в общедоступную зону.	[edit] admin@edge# set policy firewall ALL_DROP default-action drop
Фиксация настройки.	[edit] admin@edge# commit
Вывод настройки межсетевого экрана.	[edit] admin@edge# show policy firewall ALL_DROP default-action drop description "drop all traffic"

Применение базовых политик фильтрации

После создания базовых политик фильтрации необходимо определить между какими зонами они будут применяться. Необходимо помнить, что политики применяются для трафика, входящего в определенную зону. То есть для такого трафика, который передается из зоны A в зону B, для конфигурации, выглядящей следующим образом:

```
[edit]
admin@edge# show zone-policy zone B
   from A {
       policy {
           firewall A-to-B
       }
   }
```

При этом настройка ответного трафика, из зоны B в зону A настраивается в узле конфигурации, относящемуся к зоне A.

```
[edit]
admin@edge# show zone-policy zone A
   from B {
       policy {
           firewall B-to-A
       }
   }
```

Для наглядности направление трафика, к которому будут применены базовые политики представлено на рисунке 46.

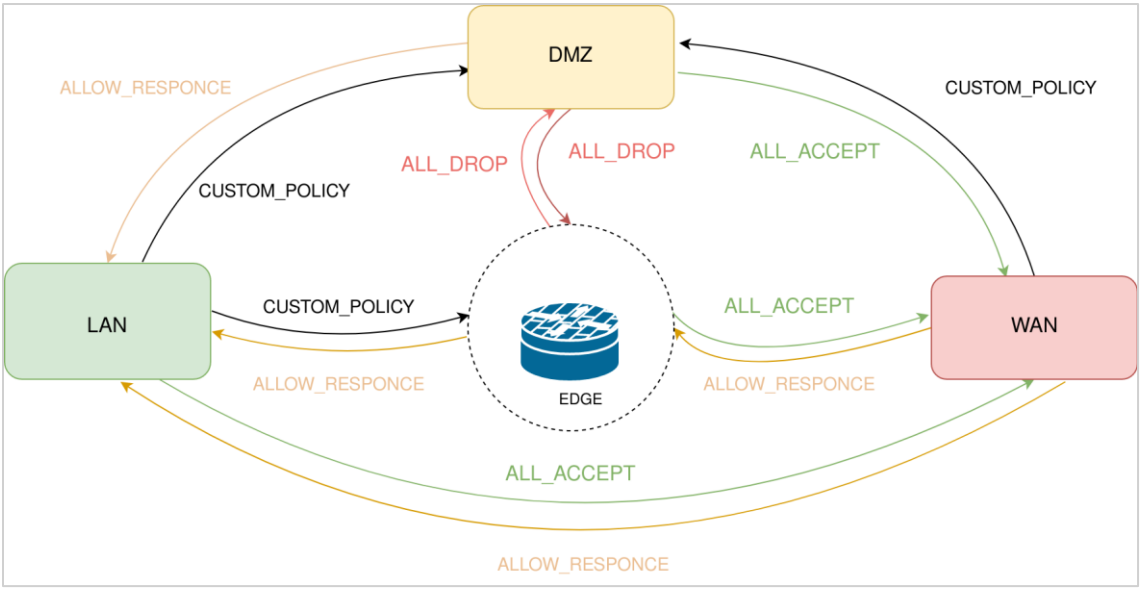


Рисунок 46 — Схема применения политик между зонами

Согласно данному рисунку получается следующий набор базовых политик фильтрации трафика:

- Разрешен весь трафик LAN-to-WAN, EDGE-to-WAN, DMZ-to-WAN.
- Разрешен только ответный трафик WAN-to-LAN, EDGE-to-LAN, WAN-to-EDGE, DMZ-to-LAN.
- Запрещен весь трафик DMZ-to-EDGE, EDGE-to-DMZ.

Для направления трафика, который помечен как CUSTOM_POLICY будут применены более сложные правила фильтрации. Настройка этих правил описана далее в документе.

Для применения настроенных политик фильтрации воспользуйтесь командами ниже.

Пример 191 – Применение базовых политик фильтрации

Действие	**Команда**
Разрешение передачи любого трафика из зоны LAN в зону WAN.	`[edit]` `admin@edge# set zone-policy zone WAN from LAN policy firewall ALL_ACCEPT`
Разрешение передачи любого трафика из локальной зоны EDGE в зону WAN.	`[edit]` `admin@edge# set zone-policy zone WAN from EDGE`

Действие	Команда
	policy firewall ALL_ACCEPT
Разрешение передачи любого трафика из зоны DMZ в зону WAN.	[edit] admin@edge# set zone-policy zone WAN from DMZ policy firewall ALL_ACCEPT
Разрешение только ответного трафика из зоны WAN в зону LAN.	[edit] admin@edge# set zone-policy zone LAN from WAN policy firewall ALLOW_RESPONSE
Разрешение только ответного трафика из локальной зоны EDGE в зону LAN.	[edit] admin@edge# set zone-policy zone LAN from EDGE policy firewall ALLOW_RESPONSE
Разрешение только ответного трафика из зоны WAN в локальную зону EDGE.	[edit] admin@edge# set zone-policy zone EDGE from WAN policy firewall ALLOW_RESPONSE
Разрешение только ответного трафика из зоны DMZ в зону LAN.	[edit] admin@edge# set zone-policy zone LAN from DMZ policy firewall ALLOW_RESPONSE
Запрет любого трафика из локальной зоны EDGE в зону DMZ.	[edit] admin@edge# set zone-policy zone DMZ from EDGE policy firewall ALL_DROP
Запрет любого трафика из зоны DMZ в локальную зону EDGE.	[edit] admin@edge# set zone-policy zone EDGE from DMZ policy firewall ALL_DROP
Применение конфигурации.	[edit] admin@edge# commit

Просмотр примененной конфигурации.	admin@edge# show zone-policy
	  zone DMZ {
	  description "DMZ ZONE"
	  from EDGE {
	  policy {
	  firewall ALL_DROP
	  }
	  }
	  interface eth2
	  }
	  zone EDGE {
	  description "Numa Edge local zone"
	  from DMZ {
	  policy {
	  firewall ALL_DROP
	  }
	  }
	  from WAN {
	  policy {
	  firewall ALLOW_RESPONSE
	  }
	  }
	  local-zone
	  }
	  zone LAN {
	  description "LAN ZONE"
	  from DMZ {
	  policy {
	  firewall ALLOW_RESPONSE
	  }
	  }
	  from EDGE {
	  policy {
	  firewall ALLOW_RESPONSE
	  }
	  }
	  from WAN {
	  policy {

Действие	Команда

	firewall ALLOW_RESPONSE
	}
	}
	interface eth3
	interface eth4
	}
	zone WAN {
	description "WAN ZONE"
	from DMZ {
	policy {
	firewall ALL_ACCEPT
	}
	}
	from EDGE {
	policy {
	firewall ALL_ACCEPT
	}
	}
	from LAN {
	policy {
	firewall ALL_ACCEPT
	}
	}
	interface eth1
	}

Создание и применение специальных политик фильтрации

Теперь создаются более сложные политики фильтрации, описывающие прохождения трафика в следующих направлениях:

- WAN-to-DMZ — политика, разрешающая доступ из интернета с помощью протоколов HTTP,HTTPS на сервер в зоне DMZ. Дополнительно разрешается весь ICMP трафик.
- LAN-to-DMZ — политика, разрешающая доступ из зоны LAN в зону DMZ с помощью протоколов HTTP и HTTPS а так же FTP и SSH . Весь ICMP трафик так же разрешен.
- LAN-to-EDGE — политика, разрешающая доступ с помощью протокола SSH только для определенного адреса отправителя.

Первоначально создадим необходимые фильтры:

- WAN_SERVICE_PORT — перечень портов, доступ к которым разрешен из публичной сети (в данном случае из зоны WAN).
- LAN_SERVICE_PORT — порты, доступ к которым разрешен из частной сети (зоны LAN).
- ICMP — фильтр, описывающий ICMP трафик.

Пример 192 – Создание фильтра WAN_SERVICE_PORT

Действие	Команда
Вначале создаем порт-группу, в которую добавляются все необходимые порты. Данный метод удобнее простого описания списка портов в правиле фильтрации, поскольку позволяет гибко управлять содержимым группы без необходимости редактирования фильтра.	[edit] admin@edge# set groups port-group PUBLIC_SERVICE_PORT port http [edit] admin@edge# set groups port-group PUBLIC_SERVICE_PORT port https
Теперь создается фильтр WAN_SERVICE_PORT, для которого в качестве портов назначения трафика выбирается ранее созданная группа.	[edit] admin@edge# set filter WAN_SERVICE_PORT rule 10 destination port-group PUBLIC_SERVICE_PORT
Синтаксис системы конфигурации требует не только указание числового или символьного обозначения	[edit] admin@edge# set filter WAN_SERVICE_PORT rule 10 protocol tcp

Действие	Команда
портов, но и протокол, относящийся к данным портам. В данном случае порты HTTP и HTTPS работают поверх протокола TCP.	
Теперь создается описание для данного фильтра.	[edit] admin@edge# set filter WAN_SERVICE_PORT description "Ports to which connections can be established from an WAN zone"
Применение конфигурации.	[edit] admin@edge# commit

Просмотр получившейся конфигурации.	[edit]
	admin@edge# show groups port-group PUBLIC_SERVICE_PORT
	  port http
	  port https
	[edit]
	admin@edge# show filter WAN_SERVICE_PORT
	  description "Ports to which connections can be established from an WAN zone"
	  rule 10 {
	  destination {
	  port-group PUBLIC_SERVICE_PORT
	  }
	  protocol tcp
	  }
	[edit]

Аналогичным образом создается правило фильтрации для доступа к сервисным портам из зоны LAN.

Пример 193 – Создание фильтра LAN_SERVICE_PORT

Действие	Команда
Аналогично с предыдущим примером создается порт-группа PRIVATE_SERVICE_PORT в которую помимо портов HTTP и HTTPS добавляются еще порты FTP и SSH.	[edit] admin@edge# set groups port-group PRIVATE_SERVICE_PORT port http [edit] admin@edge# set groups port-group PRIVATE_SERVICE_PORT port https [edit] admin@edge# set groups port-group PRIVATE_SERVICE_PORT port ftp [edit] admin@edge# set groups port-group PRIVATE_SERVICE_PORT port ssh
Также, аналогично предыдущему примеру создается правило фильтрации LAN_SERVICE_PORT, в которое добавляется данная группа.	[edit] admin@edge# set filter LAN_SERVICE_PORT rule 10 destination port-group PRIVATE_SERVICE_PORT
Все порты работают поверх протокола TCP.	[edit] admin@edge# set filter LAN_SERVICE_PORT rule 10 protocol tcp
Аналогичным образом создается описание.	[edit] admin@edge# set filter LAN_SERVICE_PORT description "Ports to which connections can be established from an LAN zone"
И полученная конфигурация применяется.	[edit] admin@edge# commit

Просмотр получившейся конфигурации.	[edit]
	admin@edge# show groups port-group PRIVATE_SERVICE_PORT
	  port http
	  port https

Действие	Команда

	port ftp
	port ssh
	
	[edit]admin@edge# show filter LAN_SERVICE_PORT
	description "Ports to which connections can be established from an LAN zone"
	rule 10 {
	destination {
	port-group PRIVATE_SERVICE_PORT
	}
	protocol tcp
	}

И последним этапом в настройке фильтров будет описание ICMP трафика.

Пример 194 – Фильтр для ICMP трафика

Действие	Команда
В качестве используемого протокола выбирается ICMP трафик.	[edit] admin@edge# set filter ICMP rule 10 protocol icmp
Для ICMP трафика выбирается любой тип сообщений. Детальная настройка разрешений для ICMP трафика выходит за рамки данного документа.	[edit] admin@edge# set filter ICMP rule 10 icmp type any
Добавление описания для фильтра.	[edit] admin@edge# set filter ICMP description "All ICMP traffic"
Применение изменений.	[edit] admin@edge# commit

Просмотр получившегося фильтра.	[edit]
	admin@edge# show filter ICMP description "All ICMP traffic" rule 10 {
	icmp {
	type any
	}
	protocol icmp
	}
	[edit]

После того как требуемые фильтры были созданы, осталось применить их к политикам фильтрации трафика между зонами.

Первоначально описывается политика, регулирующая доступ из зоны WAN в зону DMZ.

Пример 195 – Настройка политики WAN-to-DMZ

Действие	Команда
Создание политики межсетевого экранирования WAN-to-DMZ и добавления правила 10, в котором в качестве портов назначения указаны HTTP и HTTPS.	[edit] admin@edge# set policy firewall WAN-to-DMZ rule 10 match filter WAN_SERVICE_PORT
Если трафик попадает под данный фильтр, то он разрешается.	[edit] admin@edge# set policy firewall WAN-to-DMZ rule 10 action accept
Создание правила 20, в котором описан ICMP трафик.	[edit] admin@edge# set policy firewall WAN-to-DMZ rule 20 match filter ICMP
Аналогично, разрешается ICMP трафик.	[edit] admin@edge# set policy firewall WAN-to-DMZ rule 20 action accept

Действие	Команда
К трафику, который не попадает по созданные правила, применяется стандартное действие drop. Для логирования этого трафика, добавляется соответствующая настройка.	[edit] admin@edge# set policy firewall WAN-to-DMZ enable-default-log
К созданной политике межсетевого экранирования добавляется описание.	[edit] admin@edge# set policy firewall WAN-to-DMZ description "Allow only destanation HTTP,HTTPS and ICMP traffic"
Применение изменений.	[edit] admin@edge# commit

Вывод настройки политики WAN-to-DMZ.	[edit]
	admin@edge# show policy firewall WAN-to-DMZ
	  description "Allow only destanation HTTP,HTTPS and ICMP traffic"
	  enable-default-log
	  rule 10 {
	  action accept
	  match {
	  filter WAN_SERVICE_PORT
	  }
	  }
	  rule 20 {
	  action accept
	  match {
	  filter ICMP
	  }
	  }

Применение политики межсетевого экранирования, для трафика передаваемого из зоны WAN в зону DMZ.	[edit] admin@edge# set zone-policy zone DMZ from WAN policy firewall WAN-to-DMZ
Применение конфигурации.	[edit] admin@edge# commit

Теперь описывается политика межсетевого экранирования для трафика, передаваемого из зоны LAN в зону DMZ.

Пример 196 – Настройка политики LAN-to-DMZ

Действие	Команда
Аналогично предыдущему примеру создается политика LAN-to-DMZ, где в правиле 10 описывается трафик, который предназначен для служб SSH, FPT, HTTP и HTTPS.	[edit] admin@edge# set policy firewall LAN-to-DMZ rule 10 match filter LAN_SERVICE_PORT
Трафик, попадающий под это правило разрешается.	[edit] admin@edge# set policy firewall LAN-to-DMZ rule 10 action accept
Правило 20 соответствует прошлому примеру.	[edit] admin@edge# set policy firewall LAN-to-DMZ rule 20 match filter ICMP
Трафик, попадающий под это правило разрешается.	[edit] admin@edge# set policy firewall LAN-to-DMZ rule 20 action accept
Аналогично прошлому примеру, весь трафик, не попадающий под разрешающие правила – запрещается, а запись о нем заносится в системный журнал.	[edit] admin@edge# set policy firewall LAN-to-DMZ enable-default-log
Для данной политики задается описание.	[edit] admin@edge# set policy firewall LAN-to-DMZ description "Allow only destanation

Действие	Команда
	HTTP,HTTPS,FTP,SSH and ICMP traffic"
Изменения применяются.	[edit] admin@edge# commit

Вывод полученной конфигурации	[edit]
	admin@edge# show policy firewall LAN-to-DMZ
	description "Allow only destanation HTTP,HTTPS,FTP,SSH and ICMP traffic"
	enable-default-log
	rule 10 {
	action accept
	match {
	filter LAN_SERVICE_PORT
	}
	}
	rule 20 {
	action accept
	match {
	filter ICMP
	}
	}

Применение политики межсетевого экранирования, для трафика передаваемого из зоны LAN в зону DMZ.	[edit] admin@edge# set zone-policy zone DMZ from LAN policy firewall LAN-to-DMZ
Применение изменений.	[edit] admin@edge# commit

Завершающим этапом настройки будет ограничения доступа к Numa Edge из зоны LAN. Данная настройка несет потенциальный риск потерять управления в случае ошибочных действий. Для примера доступ по SSH разрешен только с устройства 10.10.1.100.

Пример 197 – Настройка политики LAN-to-EDGE

Действие	Команда
Создание политики фильтрации, который описывает возможность подключения к Numa Edge через протокол SSH только с устройства 10.10.1.100. В дальнейшем, можно использовать группу адресов для описания нескольких устройств, с которых возможно управление.	[edit] admin@edge# set filter EDGE-MGMT rule 10 destination port ssh[edit] admin@edge# set filter EDGE-MGMT rule 10 protocol tcp [edit] admin@edge# set filter EDGE-MGMT rule 10 source address 10.10.1.100
Применение изменений.	[edit] admin@edge# commit
Создание политики межсетевого экранирования, правило которого ограничивает доступ к Numa Edge.	[edit] admin@edge# set policy firewall LAN-to-EDGE rule 10 match filter EDGE-MGMT
Трафик, попадающий под это правило разрешается.	[edit] admin@edge# set policy firewall LAN-to-EDGE rule 10 action accept
Аналогично предыдущему примеру, разрешается ICMP трафик.	[edit] admin@edge# set policy firewall LAN-to-EDGE rule 20 match filter ICMP [edit] admin@edge# set policy firewall LAN-to-EDGE rule 20 action accept
Весь явно не разрешенный трафик запрещен и запись о нем заносится в системный журнал	[edit] admin@edge# set policy firewall LAN-to-EDGE enable-default-log
Для данной политики задается описание.	[edit] admin@edge# set policy firewall LAN-to-

Действие	Команда
	EDGE description "Allow SSH connection only from 10.10.1.100"
Изменения применяются.	[edit] admin@edge# commit

Просмотр изменений.	[edit]
	admin@edge# show policy firewall LAN-to-EDGE
	description "Allow SSH connection only from 10.10.1.100"
	enable-default-log
	rule 10 {
	action accept
	match {
	filter EDGE-MGMT
	}
	}
	rule 20 {
	action accept
	match {
	filter ICMP
	}
	}

Применение политики межсетевого экранирования, для трафика передаваемого из зоны LAN в зону локальную EDGE.	[edit] admin@edge# set zone-policy zone EDGE from LAN policy firewall LAN-to-EDGE
Применение конфигурации.	[edit] admin@edge# commit

Настройка межсетевого экрана на основе зон завершена и теперь необходимо убедится в его правильности с помощью проверки прохождения трафика.

21.3 Проверка

Конечная будут включает в себя генерацию ICMP трафика в следующих направлениях:

- Из LAN в LAN — передача трафика внутри одной зоны — должен быть разрешен.
- Из LAN в WAN — доступ в интернет для локальных пользователей — должен быть разрешен.
- Из WAN в LAN — проверка возможности установки соединения из интернета в локальную сеть — должен быть запрещен.
- Из WAN в DMZ — проверка доступности внутренних сервисов из интернета — должен быть разрешен.
- Из DMZ в EDGE — доступ из сервисной сети за сам маршрутизатор — должен быть запрещен.
- Из LAN в EDGE — проверка возможности управления устройством из локальной сети — должен быть разрешен.
- Из LAN в DMZ — проверка доступности внутренних сервисов внутри сети — должен быть разрешен .

Тест 1, результат – OK.

Из LAN в LAN , scr ip = 10.10.1.100, dst ip = 10.10.2.100

```
root@LAN1:~# ping 10.10.2.100 -c 1
PING 10.10.2.100 (10.10.2.100) 56(84) bytes of data.
64 bytes from 10.10.2.100: icmp_seq=1 ttl=63 time=1.50 ms

--- 10.10.2.100 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.502/1.502/1.502/0.000 ms
root@LAN1:~#
```

Тест 2, результат – OK.

Из LAN в WAN, src ip = 10.10.1.100, dst ip = 203.0.113.254

```
root@LAN1:~# ping 203.0.113.254  -c 1
PING 203.0.113.254 (203.0.113.254) 56(84) bytes of data.
64 bytes from 203.0.113.254: icmp_seq=1 ttl=63 time=1.37 ms

--- 203.0.113.254 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.373/1.373/1.373/0.000 ms
root@LAN1:~#
```

Тест 3, результат – OK.

Из WAN в LAN, src ip = 203.0.113.1 dst ip = 10.10.2.100

```
root@WAN:~# ping 10.10.2.100 -c 1
PING 10.10.2.100 (10.10.2.100) 56(84) bytes of data.

--- 10.10.2.100 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
root@WAN:~#
```

Тест 4, результат – OK.

Из WAN в DMZ, src ip = 203.0.113.254 dst ip = 172.16.0.100

```
root@WAN:~# ping 172.16.0.100 -c 1
PING 172.16.0.100 (172.16.0.100) 56(84) bytes of data.
64 bytes from 172.16.0.100: icmp_seq=1 ttl=63 time=1.47 ms

--- 172.16.0.100 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.466/1.466/1.466/0.000 ms
```

Тест 5, результат – OK.

Из DMZ в EDGE, src ip = 172.16.0.100 dst ip = 172.16.0.254

```
root@DMZ:~# ping 10.10.1.254 -c 1
PING 10.10.1.254 (10.10.1.254) 56(84) bytes of data.

--- 10.10.1.254 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

root@DMZ:~#
```

Тест 6, результат – OK.

Из LAN в EDGE, src ip = 10.10.1.100 dst ip = 10.10.1.254

```
root@LAN1:~# ping 10.10.1.254 -c 1
PING 10.10.1.254 (10.10.1.254) 56(84) bytes of data.
64 bytes from 10.10.1.254: icmp_seq=1 ttl=64 time=0.720 ms

--- 10.10.1.254 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.720/0.720/0.720/0.000 ms
```

Тест 7, результат – OK.

Из LAN в DMZ, src ip = 10.10.1.100 dst ip = 172.16.1.100

```
root@LAN1:~# ping 172.16.0.100 -c 1
PING 172.16.0.100 (172.16.0.100) 56(84) bytes of data.
64 bytes from 172.16.0.100: icmp_seq=1 ttl=63 time=1.40 ms

--- 172.16.0.100 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.404/1.404/1.404/0.000 ms
```

Дополнительно проверяется возможность подключения к Numa Edge:

Тест 8, результат – ОК.

Из LAN в Edge, src ip = 10.10.1.100 dst ip = 10.10.1.254, SSH

```
root@LAN1:~# ssh admin@10.10.1.254
The authenticity of host '10.10.1.254 (10.10.1.254)' can't be established.
ECDSA key fingerprint is SHA256:tgO+iGtDZ8imoF7Oh4QtrSm7HaSkqnmZQpxxgeWi+Ew.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.1.254' (ECDSA) to the list of known hosts.
Numa Edge 1.0
Password:
```

Тест 9, результат – ОК.

Из LAN в Edge, src ip = 10.10.2.100 dst ip = 10.10.2.254, SSH

```
root@LAN2:~# ssh admin@10.10.2.254
ssh: connect to host 10.10.2.254 port 22: Connection timed out
```

После проверки рекомендуется сохранить конфигурацию, чтобы она была доступна после перезагрузки устройства. Для этого выполните команду:

```
[edit]
admin@edge# save
```

21.4 Команды межсетевого экрана на основе зон

Команды настройки	
zone-policy zone <зона-получатель>	Определение зоны безопасности.
zone-policy zone <зона-получатель> default-action <действие>	Определение действия по умолчанию для трафика, приходящего в зону безопасности.
zone-policy zone <зона-получатель> description <описание>	Ввод описания для зоны безопасности.
zone-policy zone <зона-получатель> from <зона-отправитель>	Определение имени зоны-источника трафика, к которому применяется данная политика.
zone-policy zone <зона-получатель> from <зона-отправитель> policy <тип_политики> <имя>	Применение указанной политики к трафику, приходящему из указанной зоны-“отправителя”.
zone-policy zone <зона-получатель> interface <имя_интерфейса>	Добавление интерфейса в зону безопасности.
zone-policy zone <зона-получатель> local-zone	Выделение зоны в качестве “локальной”.

21.4.1 zone-policy zone <зона-получатель>

Определение зоны безопасности.

Синтаксис

```
set zone-policy zone <зона-получатель>
delete zone-policy zone <зона-получатель>
show zone-policy zone
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
zone-policy {
    zone зона-получатель {
    }
}
```

Параметры

зона-получатель

Множественный узел. Название зоны безопасности. Можно определить несколько зон безопасности, создав несколько узлов конфигурации zone-policy zone**.**

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для создания зоны безопасности.

В Numa Edge зона определяется как группа интерфейсов с одинаковым уровнем безопасности. После определения зоны к трафику, передаваемому между зонами, можно применить политику фильтрации. По умолчанию трафик в зону игнорируется, если не определена политика для зоны, отправляющей трафик. Трафик, передаваемый внутри зоны, не фильтруется. При определении зон следует помнить следующие моменты.

- Интерфейс может быть членом только одной зоны.
- К интерфейсу, являющемуся членом зоны, не может быть непосредственно применена политика межсетевого экранирования.
- Трафик на интерфейсах, не приписанных к зоне, по умолчанию не фильтруется. К этим интерфейсам могут быть непосредственно применены наборы правил.

Форма **set** этой команды используется для определения зоны безопасности.

Форма **delete** этой команды используется для удаления зоны безопасности.

Форма **show** этой команды используется для просмотра настройки зоны безопасности.

21.4.2 zone-policy zone <зона-получатель> default-action <действие>

Определение действия по умолчанию для трафика, приходящего в зону безопасности.

Синтаксис

```
set zone-policy zone <зона-получатель> default-action <действие>
delete zone-policy zone <зона-получатель> default-action
show zone-policy zone <зона-получатель> default-action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
zone-policy {
    zone зона-получатель {
        default-action действие
    }
}
```

Параметры

зона-получатель

Множественный узел. Название зоны безопасности. Можно определить несколько зон безопасности, создав несколько узлов конфигурации zone-policy zone**.**

действие

Действие, которое должно быть выполнено для трафика, приходящего в зону безопасности. Допустимые значения:

- **accept:** Трафик разрешен;
- **drop:** Трафик игнорируется без каких-либо действий и сообщений;
- **reject:** Трафик игнорируется с выдачей сообщения ICMP о недоступности.

Значение по умолчанию

Трафик игнорируется без каких-либо действий и сообщений.

Указания по использованию

Эта команда используется для указания действия по умолчанию в отношении трафика, приходящего в зону безопасности. Это действие, которое будет выполнено для всего трафика, приходящего из зон, для которых политика не определена. Это означает, что если необходимо разрешить прохождение трафика из определенной зоны, то необходимо явно определить политику, разрешающую прохождение трафика из этой зоны.

Форма **set** этой команды используется для установки действия по умолчанию.

Форма **delete** этой команды используется для восстановления поведения по умолчанию.

Форма **show** этой команды используется для просмотра настройки действия по умолчанию.

21.4.3 zone-policy zone <зона-получатель> description <описание>

Ввод описания для зоны безопасности.

Синтаксис

```
set zone-policy zone <зона-получатель> description <описание>
delete zone-policy zone <зона-получатель> description
show zone-policy zone <зона-получатель> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
zone-policy {
   zone зона-получатель {
      description описание
   }
}
```

Параметры

зона-получатель

Множественный узел. Название зоны безопасности. Можно определить несколько зон безопасности, создав несколько узлов конфигурации zone-policy zone**.**

описание

Строка, содержащая краткое описание зоны безопасности. Если в строке есть пробелы, её следует заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для записи краткого описания зоны безопасности.

Форма **set** этой команды используется для ввода описания.

Форма **delete** этой команды используется для удаления описания.

Форма **show** этой команды используется для просмотра настройки описания.

21.4.4 zone-policy zone <зона-получатель> from <зона-отправитель>

Определение имени зоны-источника трафика, к которому применяется данная политика.

Синтаксис

```
set zone-policy zone <зона-получатель> from <зона-отправитель>
delete zone-policy zone <зона-получатель> from <зона-отправитель>
show zone-policy zone <зона-получатель> from
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
zone-policy {
   zone зона-получатель {
      from зона-отправитель {
      }
   }
}
```

Параметры

зона-получатель

Множественный узел. Название зоны безопасности. Можно определить несколько зон безопасности, создав несколько узлов конфигурации zone-policy zone**.**

зона-отправитель

Имя зоны, из которой приходит трафик.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания зоны, из которой будет приходить трафик (зоны-“отправителя”). Политика фильтрации пакетов для этой зоны-“отправителя” применяется ко всему трафику, приходящему из этой зоны.

Форма **set** этой команды используется для ввода описания.

Форма **delete** этой команды используется для удаления описания.

Форма **show** этой команды используется для просмотра настройки описания.

21.4.5 zone-policy zone <зона-получатель> from <зона-отправитель> policy <тип_политики> <имя>

Применение указанной политики к трафику, приходящему из указанной зоны-“отправителя”.

Синтаксис

```
set zone-policy zone <зона-получатель> from <зона-отправитель> policy <тип_политики> <имя>

delete zone-policy zone <зона-получатель from <зона-отправитель> policy <тип_политики> [<имя>]

show zone-policy zone <зона-получатель from <зона-отправитель> policy <тип_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
zone-policy {
    zone зона-получатель {
        from зона-отправитель {
            policy {
                тип_политики имя
            }
        }
    }
}
```

Параметры

зона-получатель

Множественный узел. Название зоны безопасности. Можно определить несколько зон безопасности, создав несколько узлов конфигурации zone-policy zone.*зона-отправитель*

Имя зоны, из которой приходит трафик.

тип_политики

Указывает тип политики, применяемый к трафику из указанной зоны. Допустимые значения представлены в таблице ниже.

Таблица 177 – Допустимые типы политик для трафика между зонами.

Значение	Описание
clone	Политика клонирования трафика IPv4
clone-ipv6	Политика клонирования трафика IPv6
firewall	Политика межсетевого экранирования IPv4
firewall-ipv6	Политика межсетевого экранирования IPv6
modify	Политика модификации трафика IPv4
modify-ipv6	Политика модификации трафика IPv6

Для зоны-“отправителя” можно применить одну политику для IPv4 и одну – для IPv6.

имя

Имя политики указанного типа, которая применяется к трафику от зоны-"отправителя".

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для применения политик к любому трафику, приходящему из зоны-“отправителя”.

Форма **set** этой команды используется для указания политики для зоны-“отправителя”.

Форма **delete** этой команды используется для удаления политики для зоны-“отправителя”.

Форма **show** используется для вывода политик, примененных к зоне-“отправителю” (если таковые имеются).

21.4.6 zone-policy zone <зона-получатель> interface <имя_интерфейса>

Добавление интерфейса в зону безопасности.

Синтаксис

```
set zone-policy zone <зона-получатель> interface <имя_интерфейса>
delete zone-policy zone <зона-получатель> interface <имя_интерфейса>
show zone-policy zone <зона-получатель> interface
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
zone-policy {
   zone зона-получатель {
      interface имя_интерфейса
   }
}
```

Параметры

зона-получатель

Множественный узел. Название зоны безопасности. Можно определить несколько зон безопасности, создав несколько узлов конфигурации zone-policy zone**.**

имя_интерфейса

Множественный узел. Имя интерфейса, добавляемого в состав указанной зоны, например: eth0, wan1 или ppp1.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для добавления интерфейса в зону безопасности. У всех интерфейсов в зоне безопасности уровень безопасности один и тот же; трафик, приходящий на эти интерфейсы из других зон, обрабатывается одинаковым образом. Трафик, передаваемый между интерфейсами в одной зоне безопасности, не фильтруется.

Форма **set** этой команды используется для добавления интерфейса в зону.

Форма **delete** этой команды используется для удаления интерфейса из зоны.

Форма **show** этой команды используется для просмотра списка интерфейсов, являющихся членами этой зоны.

21.4.7 zone-policy zone <зона-получатель> local-zone

Выделение зоны в качестве “локальной”.

Синтаксис

```
set zone-policy zone <зона-получатель> local-zone
delete zone-policy zone <зона-получатель> local-zone
show zone-policy zone <зона-получатель>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
zone-policy {
   zone зона-получатель {
      local-zone
   }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для выделения зоны безопасности в качестве “локальной” зоны.

Локальная зона – это особая зона, относящаяся к самому локальному устройству под управлением Numa Edge. Если указать зону безопасности как локальную, то политики межсетевого экрана, указанные для этой зоны, будут фильтровать пакеты, предназначенные для самого Numa Edge. По умолчанию разрешается весь трафик, предназначенный для маршрутизатора и инициированный маршрутизатором. В качестве локальной может быть выделена только одна зона.

Форма **set** этой команды используется для выделения зоны безопасности в качестве локальной зоны.

Форма **delete** этой команды используется для прекращения использования зоны безопасности в качестве локальной зоны.

Форма **show** этой команды используется для просмотра настройки зоны безопасности.

22 QOS

22.1 Примеры настройки QoS

В данном разделе приведены следующие примеры настройки реализации качества обслуживания (QoS) в Numa Edge.

Представлены следующие примеры:

- Пример на исходящий трафик - управление загрузкой канала
- Пример на входящий трафик – ограничение трафика
- Пример на входящий трафик – контроль пропускной способности на нескольких интерфейсах
- Пример на исходящий трафик — применение иерархического QoS.

22.1.1 Пример на исходящий трафик - управление загрузкой канала

На рисунке показана простая сеть филиала с использованием QoS в Numa Edge (edge). В схеме представлен сегмент сети, у которого в качестве маршрутизатора установлен Edge. Ширина канала, предоставляемого провайдером, равна 10 Мб. Локальная сеть поделена на несколько сегментов: Серверный сегмент, Административный сегмент и Офисный сегмент.

В приведенном примере:

- весь трафик проходит по каналу шириной 10 Мбит до Интернет-провайдера;
- для трафика серверного сегмента, необходимо выделить минимум 45% пропускной способности;
- для трафика административного сегмента, необходимо выделить минимум 30% пропускной способности
- оставшиеся 25% для всего остального трафика;
- все потоки трафика будут использовать доступную пропускную способность сверх настроенных для них минимальных скоростей;

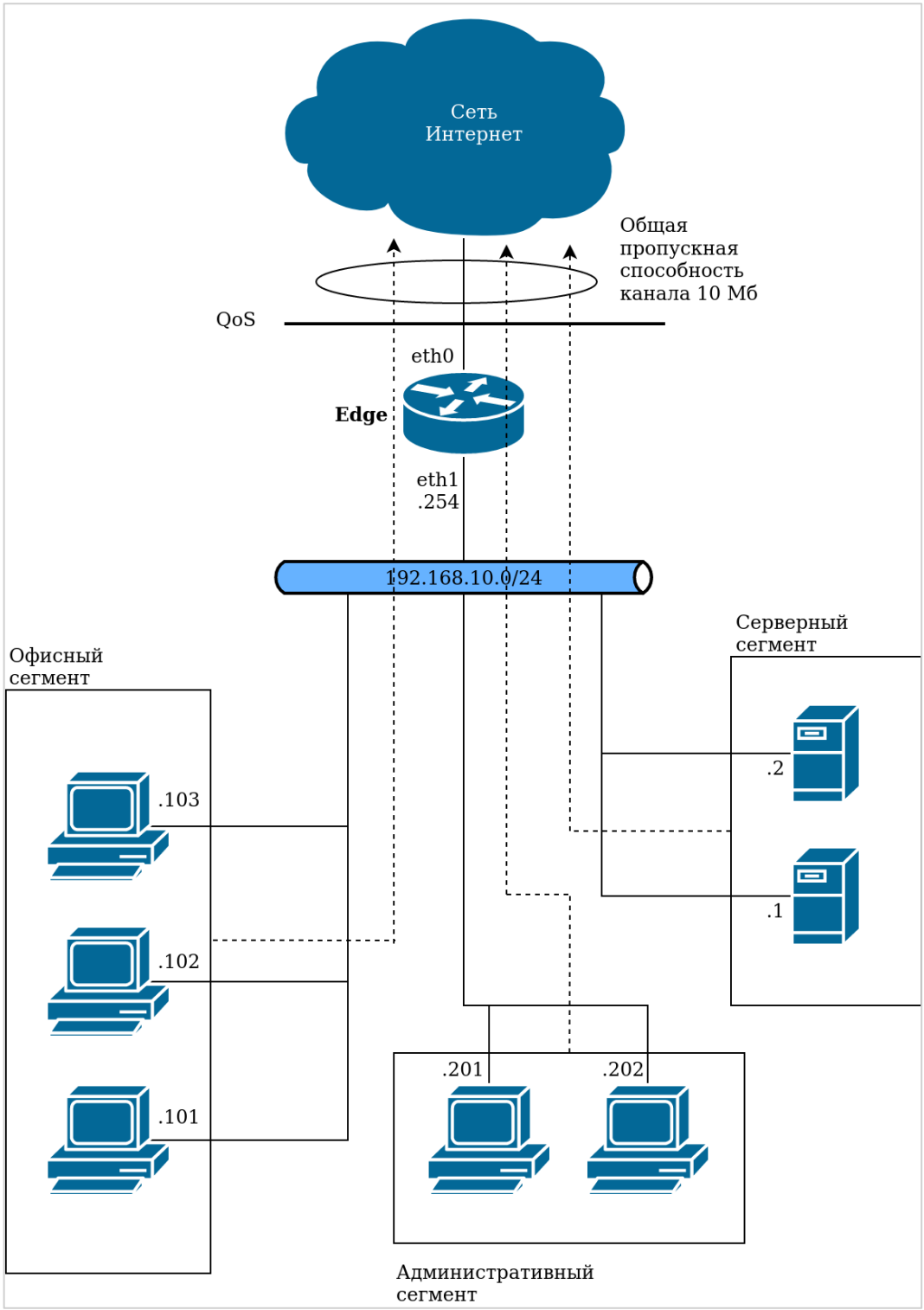


Рисунок 47 – Пример филиала с VoIP с использованием QoS

Для настройки данной схемы нужно выполнить следующие действия в режиме настройки.

Пример 198 – Управление загрузкой канала

Действие	**Команда**
Создание узла конфигурации для политики QoS.	`[edit]` `admin@edge# set policy qos shaper Lan-shape-Output`
Добавление описания.	`[edit]` `admin@edge# set policy qos shaper Lan-shape-Output description "Output shape traffic"`

Действие	**Команда**
Установка пропускной способности канала.	[edit] admin@edge# set policy qos shaper Lan-shape-Output bandwidth 10mbit
Установка пропускной способности для трафика не подходящего ни к одному из классов.	[edit] admin@edge# set policy qos shaper Lan-shape-Output default bandwidth 25%
Разрешение для трафика не подходящего ни к одному из классов, использовать всю доступную пропускную способность.	[edit] admin@edge# set policy qos shaper Lan-shape-Output default ceiling 100%
Добавление описания для трафика второго класса – данных Серверного сегмента.	[edit] admin@edge# set policy qos shaper Lan-shape-Output class 2 description "Servers segment"
Назначение пропускной способности для трафика второго класса.	[edit] admin@edge# set policy qos shaper Lan-shape-Output class 2 bandwidth 55%
Разрешение трафику второго класса использовать всю доступную пропускную способность.	[edit] admin@edge# set policy qos shaper Lan-shape-Output class 2 ceiling 100%
Добавление описания для группы адресов Серверного сегмента.	[edit] admin@edge# set groups address-group GroupServers description "Servers segment group"
Добавление в группу адресов первого сервера.	[edit] admin@edge# set groups address-group GroupServers address 192.168.10.1
Добавление в группу адресов первого сервера.	[edit] admin@edge# set groups address-group GroupServers address 192.168.10.2
Создание фильтра для определения трафика Серверного сегмента.	[edit] admin@edge# set filter QosServers rule 1 source address-group GroupServers
Фиксация изменения.	[edit] admin@edge# commit

Вывод настроек фильтра для определения данных Серверного сегмента.	[edit]
	admin@edge# show groups
	address-group GroupServers {
	address 192.168.10.1
	address 192.168.10.2
	description "Servers segment group"
	}
	[edit]
	admin@edge# show filter
	QosServers {
	rule 1 {
	source {
	address-group GroupServers
	}
	}
	}

Определение соответствия трафика на основе фильтра QosServers.	[edit] admin@edge# set policy qos shaper Lan-shape-Output class 2 match QosServers filter QosServers
Добавление описания для трафика третьего класса – данных Административного сегмента.	[edit] admin@edge# set policy qos shaper Lan-shape-Output class 3 description "Administration segment"

Действие	**Команда**
Назначение пропускной способности для трафика третьего класса.	[edit] admin@edge# set policy qos shaper Lan-shape-Output class 3 bandwidth 30%
Разрешение трафику третьего класса использовать всю доступную пропускную способность.	[edit] admin@edge# set policy qos shaper Lan-shape-Output class 3 ceiling 100%
Добавление описания для группы адресов Административного сегмента.	[edit] admin@edge# set groups address-group GroupAdministation description "Administration segment"
Добавление в группу адресов первого АРМ.	[edit] admin@edge# set groups address-group GroupAdministation address 192.168.10.201
Добавление в группу адресов второго АРМ.	[edit] admin@edge# set groups address-group GroupAdministation address 192.168.10.202
Создание фильтра для определения трафика Административного сегмента.	[edit] admin@edge# set filter QosAdministation rule 1 source address-group GroupAdministation
Фиксация изменения.	[edit] admin@edge# commit

Вывод настроек фильтра для определения данных Административного сегмента.	[edit]
	admin@edge# show groups
	address-group GroupAdministation {
	address 192.168.10.201
	address 192.168.10.202
	description "Administration segment"
	}
	admin@edge# show filter
	QosAdministation {
	rule 1 {
	source {
	address-group GroupAdministation
	}
	}
	}

Определение соответствия трафика на основе фильтра QosAdministation.	[edit] admin@edge# set policy qos shaper Lan-shape-Output class 3 match QosAdministation filter QosAdministation
Фиксация изменения.	[edit] admin@edge# commit

Вывод настройки раздела policy.	admin@edge# show policy
	qos {
	shaper Lan-shape-Output {
	bandwidth 10mbit
	class 2 {
	bandwidth 55%
	ceiling 100%
	description "Servers segment"
	match QosServers {
	filter QosServers
	}
	}
	class 3 {
	bandwidth 30%
	ceiling 100%

Действие	**Команда**

	description "Administration segment"
	match QosAdministation {
	filter QosAdministation
	}
	}
	default {
	bandwidth 25%
	ceiling 100%
	}
	description "Output shape traffic"
	}
	}

Назначение политики QoS интерфейсу, через который осуществляется подключение к Интернет-провайдеру.	[edit] admin@edge# set interfaces ethernet eth0 policy out qos Lan-shape-Output
Фиксация изменения.	[edit] admin@edge# commit

Вывод перечня политик QoS назначенных, интерфейсу, через который осуществляется подключение к Интернет-провайдеру.	[edit]
	admin@edge# show interfaces ethernet eth0 policy
	out {
	qos Lan-shape-Output
	}

22.1.2 Пример на входящий трафик – ограничение трафика

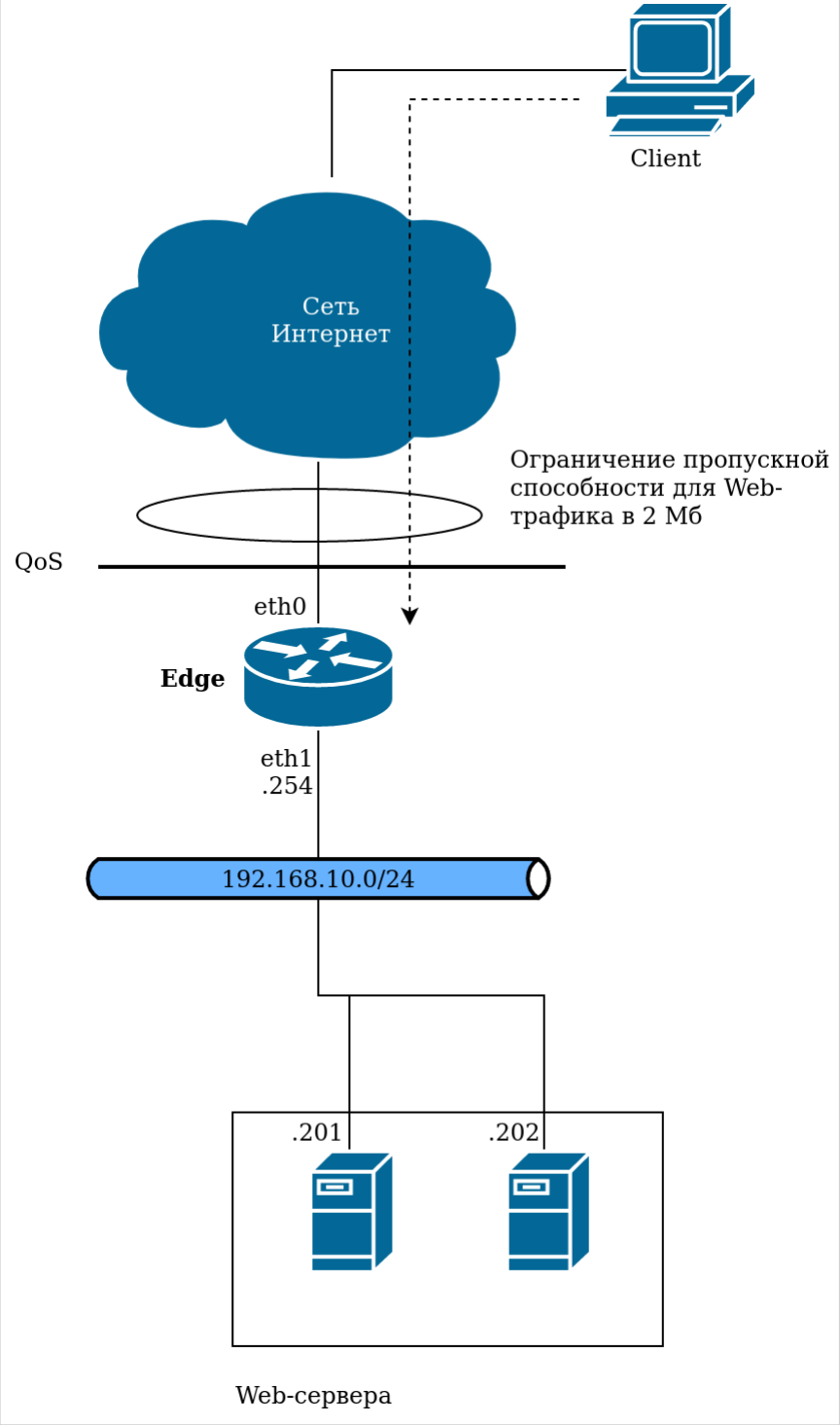


Рисунок 48 – Схема стенда

В данном примере выполняется ограничение входящего web-трафика (80 и 443 порты) до 2 Мбит/с. Для настройки данной схемы нужно выполнить следующие действия в режиме настройки.

Пример 199 – Ограничение трафика

Действие	**Команда**
Создание узла конфигурации для данной политики QoS.	`[edit]` `admin@edge# set policy qos limiter Limit-Web-Input`
Добавление описания для первого класса трафика – Веб-данных.	`[edit]` `admin@edge# set policy qos limiter Limit-`

Действие	Команда
	`Web-Input class 1 description "Input limit traffic"`
Назначение пропускной способности для первого класса.	`[edit]` `admin@edge# set policy qos limiter Limit-Web-Input class 1 bandwidth 2mbit`
Определение соответствия трафика на основе 80 порта получателя.	`[edit]` `admin@edge# set policy qos limiter Limit-Web-Input class 1 match Web-traffic ip destination port 80`
Определение соответствия трафика на основе 443 порта получателя.	`[edit]` `admin@edge# set policy qos limiter Limit-Web-Input class 1 match Web-traffic ip destination port 443`
Определение соответствия трафика на основе протокола tcp.	`[edit]` `admin@edge# set policy qos limiter Limit-Web-Input class 1 match Web-traffic ip protocol tcp`
Фиксация изменения.	`[edit]` `admin@edge# commit`

Отображение настройки policy qos.	`[edit]`
	`admin@edge# show policy qos`
	`limiter Limit-Web-Input {`
	`class 1 {`
	`bandwidth 2mbit`
	`description "Input limit traffic"`
	`match Web-traffic {`
	`ip {`
	`destination {`
	`port 80`
	`port 443`
	`protocol tcp`
	`}`
	`}`
	`}`
	`}`
	`}`

Назначение политики QoS интерфейсу, через который осуществляется подключение к Интернет-провайдеру.	`[edit]` `admin@edge# set interfaces ethernet eth0 policy in qos Limit-Web-Input`
Фиксация изменения.	`[edit]` `admin@edge# commit`

Вывод политики QoS интерфейсу, через который осуществляется подключение к Интернет-провайдеру.	`[edit]`
	`admin@edge# show interfaces ethernet eth0 policy`
	`in {`
	`qos Limit-Web-Input`
	`}`

22.1.3 Пример на входящий трафик – контроль пропускной способности на нескольких интерфейсах

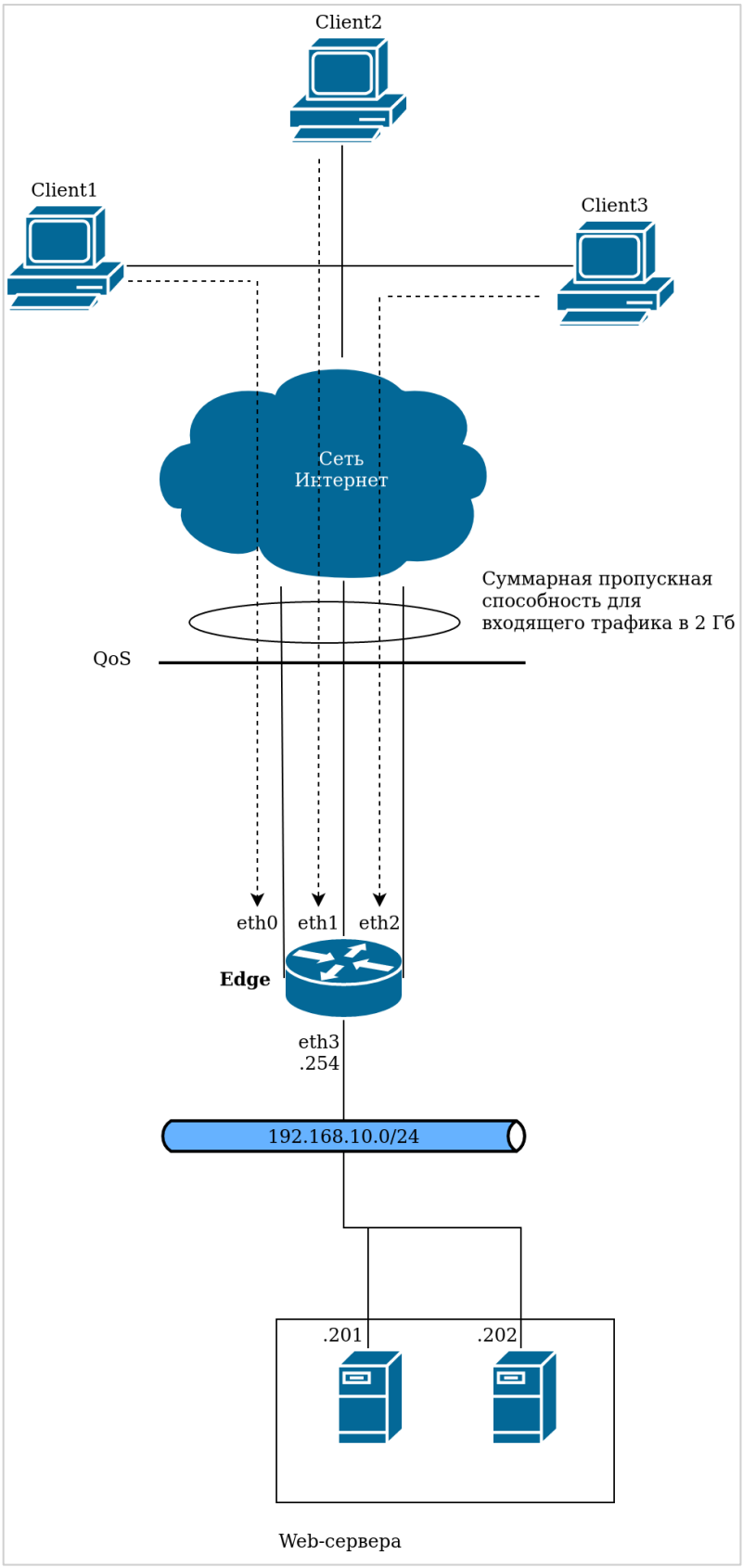


Рисунок 49 – Схема стенда

В данном примере суммарный входящий трафик с интерфейсов eth0, eth1 и eth2 не должен превосходить 2 Гбит/с. Для контроля этого ограничения входящий трафик с этих интерфейсов перенаправляется на входной

интерфейс ifb10. Создается политика контроля скорости для ограничения трафика величиной 2 Гбит/с, после чего она назначается интерфейсу ifb10.

Для настройки данной схемы нужно выполнить следующие действия в режиме настройки.

Пример 200 - Ограничение трафика на нескольких интерфейсах

Действие	**Команда**
Создание IBF-интерфейса	`[edit]` `admin@edge# set interfaces input ifb10`
Перенаправление трафика eth0 на входной интерфейс ifb10.	`[edit]` `admin@edge# set interfaces ethernet eth0 redirect ifb10`
Перенаправление трафика eth1 на входной интерфейс ifb10.	`[edit]` `admin@edge# set interfaces ethernet eth1 redirect ifb10`
Перенаправление трафика eth2 на входной интерфейс ifb10.	`[edit]` `admin@edge# set interfaces ethernet eth2 redirect ifb10`
Создание узла конфигурации для данной политики QoS.	`[edit]` `admin@edge# set policy qos rate-control Rate-Control-Input`
Добавление описания для политики QoS.	`[edit]` `admin@edge# set policy qos rate-control Rate-Control-Input description "Input rate traffic"`
Назначение ограничения пропускной способности трафику.	`[edit]` `admin@edge# set policy qos rate-control Rate-Control-Input bandwidth 2Gbit`
Фиксация изменения.	`[edit]` `admin@edge# commit`

Отображение настройки policy qos.	`[edit]`
	`admin@edge# show policy qos`
	`rate-control Rate-Control-Input {`
	`bandwidth 2Gbit`
	`description "Input rate traffic"`
	`}`

Применение политики QoS к исходящему трафику на ifb10 (состоящему из суммарного трафика с eth0, eth1 и eth2). Исходящий трафик со входного интерфейса является внутренним для устройства Numa edge.	`[edit]` `admin@edge# set interfaces input ifb10 policy out qos Rate-Control-Input`
Фиксация изменения.	`[edit]` `admin@edge# commit`

Вывод перечня политик QoS, назначенных интерфейсу ifb10.	`[edit]`
	`admin@edge# show interfaces input ifb10 policy out`
	`qos {`
	`Rate-Control-Input`
	`}`

22.1.4 Пример на исходящий трафик — применение иерархического QoS.

На рисунке показана простая сеть филиала с использованием QoS в Numa Edge (edge) для выполнения различных действий над тремя потоками трафика. На схеме представлена удаленная площадка с серверами, подключенная к Numa Edge через VPN. Локальная сеть состоит из IP-телефонии и серверного сегмента передающих данные через VPN на удаленную площадку, а также пользователей, подключающихся к Интернету.

- Весь трафик проходит по каналу 10 Мбит до Интернет-провайдера.
- Минимум 40% (4 Мбит) пропускной способности канала следует зарезервировать для трафика VPN. Из них 25% резервируются для трафика по протоколу RTP, 5% для трафика по протоколу SIP (Оба

протокола используют протоколы TCP или UDP на транспортном уровне, поэтому потоки RTP и SIP различаются по номеру порта назначения: трафик по протоколу SIP направляется на порт 5060, а трафик по протоколу RTP – на порт номер 5004). От оставшейся пропускной способности канала, 60% резервируются для трафика по протоколу TCP и 10% для всего остального трафика.

- Для трафика SIP и RTP используется алгоритм отбрасывания конца очереди. Для TCP — алгоритм справедливой очереди с указанием значения лимита пакетов в очереди равного 127.
- Остальные 60% от общей пропускной способности канала следует зарезервировать для пользователей, подключающихся к сети Интернет. Из них 7% резервируются для передачи почты на порт номер 25 (SMTP) по протоколу TCP или UDP.

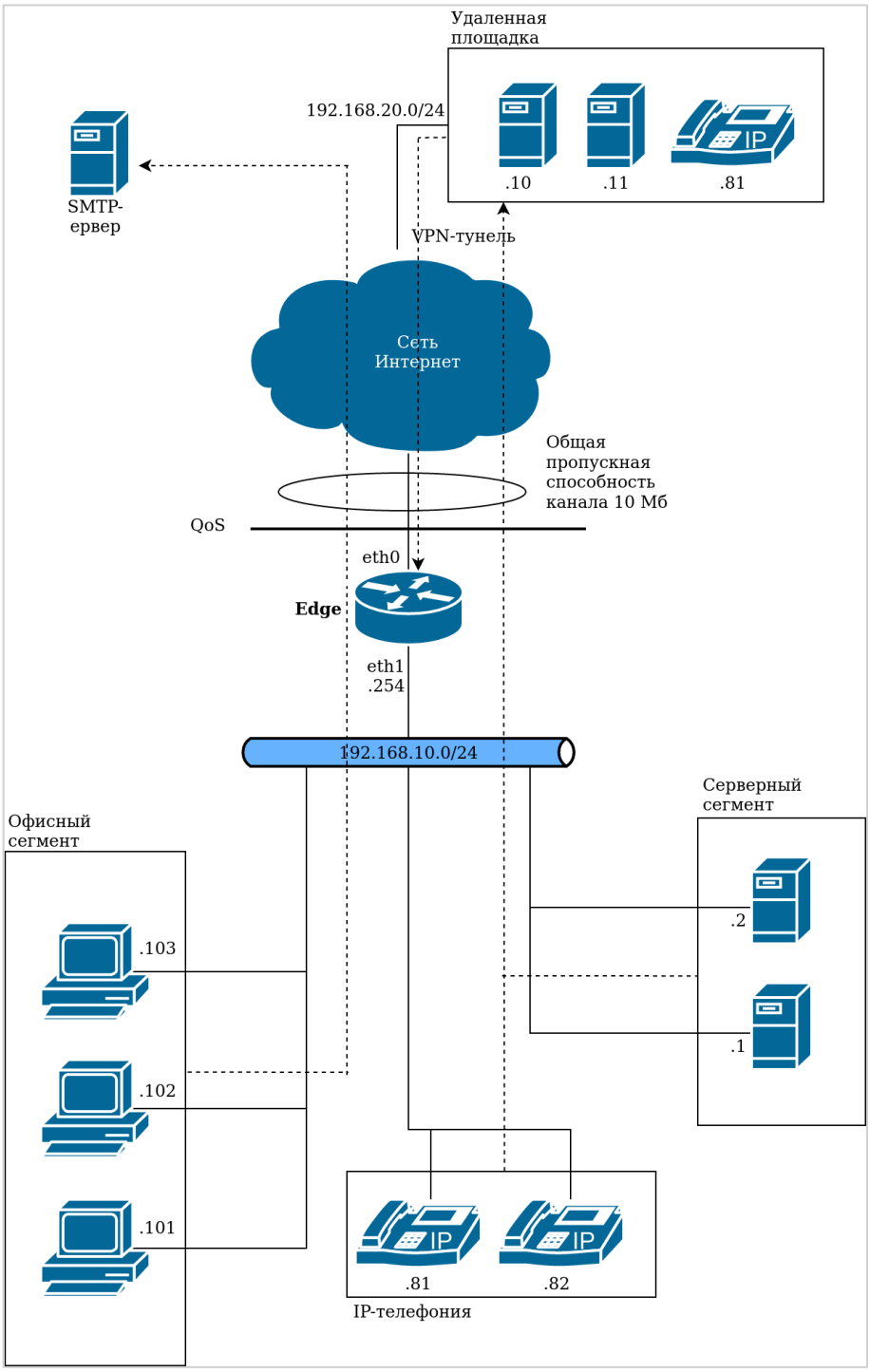


Рисунок 50 – Пример филиала с использованием QoS

Для настройки данной схемы нужно выполнить следующие действия в режиме настройки.

Пример 201 – Ограничение трафика на нескольких интерфейсах

Действие	**Команда**
Создание узла конфигурации для политики QoS.	`[edit]` `admin@edge# set policy qos shaper Shaper-Output`
Добавление описания.	`[edit]` `admin@edge# set policy qos shaper Shaper-Output description "Output shaper VPN and Internet traffic"`
Установка суммарной пропускной способности канала.	`[edit]` `admin@edge# set policy qos shaper Shaper-Output bandwidth 10mbit`
Назначение пропускной способности для Интернет трафика.	`[edit]` `admin@edge# set policy qos shaper Shaper-Output default bandwidth 60%`
Разрешение трафику по умолчанию (в данном случае это трафик сети Интернет) использовать всю доступную пропускную способность.	`[edit]` `admin@edge# set policy qos shaper Shaper-Output default ceiling 100%`
Добавление описания для трафика второго класса – трафика VPN-туннеля.	`[edit]` `admin@edge# set policy qos shaper Shaper-Output class 2 description "VPN segment"`
Назначение пропускной способности для трафика второго класса.	`[edit]` `admin@edge# set policy qos shaper Shaper-Output class 2 bandwidth 40%`
Разрешение трафику второго класса использовать всю доступную пропускную способность.	`[edit]` `admin@edge# set policy qos shaper Shaper-Output class 2 ceiling 100%`
Создание фильтра с правилом определения входящего трафика, получененого через VPN-туннеля.	`[edit]` `admin@edge# set filter VPN-traffic rule 10 source address 192.168.20.0/24`
Создание фильтра с правилом определения ихходящего трафика, предназначенного для VPN-туннеля.	`[edit]` `admin@edge# set filter VPN-traffic rule 20 destination address 192.168.20.0/24`
Фиксация изменения.	`[edit]` `admin@edge# commit`

Вывод настроек фильтра для определения данных VPN-туннеля.	`[edit]`
	`admin@edge# show filter VPN-traffic`
	`rule 10 {`
	`source {`
	`address 192.168.20.0/24`
	`}`
	`}`
	`rule 20 {`
	`destination {`
	`address 192.168.20.0/24`
	`}`
	`}`

Определение соответствия трафика второго класса на основе фильтра VPN-traffic.	`[edit]` `admin@edge# set policy qos shaper Shaper-Output class 2 match VPN-traffic filter VPN-traffic`
Создание узла конфигурации для политики QoS для трафика, передаваемого через VPN-туннель.	`[edit]` `admin@edge# set policy qos shaper Shaper-VPN-Output`
Добавление описания.	`[edit]` `admin@edge# set policy qos shaper Shaper-VPN-Output description "Output shaper SIP-RTP-TCP traffic"`

Действие	**Команда**
Установка суммарной пропускной способности канала.	`[edit]` `admin@edge# set policy qos shaper Shaper-VPN-Output bandwidth auto`
Назначение пропускной способности для трафика по умолчанию.	`[edit]` `admin@edge# set policy qos shaper Shaper-VPN-Output default bandwidth 10%`
Разрешение трафику по умолчанию использовать всю доступную пропускную способность.	`[edit]` `admin@edge# set policy qos shaper Shaper-VPN-Output default ceiling 100%`
Добавление описания для трафика второго класса – SIP-трафика.	`[edit]` `admin@edge# set policy qos shaper Shaper-VPN-Output class 2 description "SIP-traffic"`
Назначение пропускной способности для трафика второго класса.	`[edit]` `admin@edge# set policy qos shaper Shaper-VPN-Output class 2 bandwidth 5%`
Разрешение трафику второго класса использовать всю доступную пропускную способность.	`[edit]` `admin@edge# set policy qos shaper Shaper-VPN-Output class 2 ceiling 100%`
Определение политики с отбрасыванием конца очереди для трафика второго класса.	`[edit]` `admin@edge# set policy qos shaper Shaper-VPN-Output class 2 queue-type drop-tail`
Создание фильтра с правилом определения SIP-трафика (по протоколам TCP и UDP).	`[edit]` `admin@edge# set filter SIP-traffic rule 10 protocol tcp_udp`
Добавление к фильтру правила определения исходящего SIP-трафика на порт 5060.	`[edit]` `admin@edge# set filter SIP-traffic rule 10 source port 5060`
Создание фильтра с правилом определения SIP-трафика (по протоколам TCP и UDP).	`[edit]` `admin@edge# set filter SIP-traffic rule 20 protocol tcp_udp`
Добавление к фильтру правила определения входящего SIP-трафика на порт 5060.	`[edit]` `admin@edge# set filter SIP-traffic rule 20 destination port 5060`
Фиксация изменения.	`[edit]` `admin@edge# commit`

Вывод настроек фильтра для определения SIP-трафика.	`[edit]`
	`admin@edge# show filter SIP-traffic`
	`rule 10 {`
	`protocol tcp_udp`
	`source {`
	`port 5060`
	`}`
	`}`
	`rule 20 {`
	`destination {`
	`port 5060`
	`}`
	`protocol tcp_udp`
	`}`

Определение соответствия трафика второго класса на основе фильтра SIP-traffic.	`[edit]` `admin@edge# set policy qos shaper Shaper-VPN-Output class 2 match SIP-traffic filter SIP-traffic`
Добавление описания для трафика третьего класса – RTP-трафика.	`[edit]` `admin@edge# set policy qos shaper Shaper-VPN-Output class 3 description "RTP-traffic"`

Действие	**Команда**
Назначение пропускной способности для трафика третьего класса.	[edit] admin@edge# set policy qos shaper Shaper-VPN-Output class 3 bandwidth 25%
Разрешение трафику третьего использовать всю доступную пропускную способность.	[edit] admin@edge# set policy qos shaper Shaper-VPN-Output class 3 ceiling 100%
Определение алгоритма с отбрасыванием конца очереди для трафика третьего класса.	[edit] admin@edge# set policy qos shaper Shaper-VPN-Output class 3 queue-type drop-tail
Создание фильтра с правилом определения RTP-трафика (по протоколам TCP и UDP).	[edit] admin@edge# set filter RTP-traffic rule 10 protocol tcp_udp
Добавление к фильтру правила определения исходящего RTP-трафика на порт 5004.	[edit] admin@edge# set filter RTP-traffic rule 10 source port 5004
Создание фильтра с правилом определения RTP-трафика (по протоколам TCP и UDP).	[edit] admin@edge# set filter RTP-traffic rule 20 protocol tcp_udp
Добавление к фильтру правила определения входящего RTP-трафика на порт 5004.	[edit] admin@edge# set filter RTP-traffic rule 20 destination port 5004
Фиксация изменения.	[edit] admin@edge# commit

Вывод настроек фильтра для определения RTP-трафика.	[edit]
	admin@edge# show filter RTP-traffic
	rule 10 {
	protocol tcp_udp
	source {
	port 5004
	}
	}
	rule 20 {
	destination {
	port 5004
	}
	protocol tcp_udp
	}

Определение соответствия трафика третьего класса на основе фильтра RTP-traffic.	[edit] admin@edge# set policy qos shaper Shaper-VPN-Output class 3 match RTP-traffic filter RTP-traffic
Добавление описания для трафика четвертого класса – TCP-трафика.	[edit] admin@edge# set policy qos shaper Shaper-VPN-Output class 4 description "TCP-traffic"
Назначение пропускной способности для трафика четвертого класса.	[edit] admin@edge# set policy qos shaper Shaper-VPN-Output class 4 bandwidth 60%
Разрешение трафику четвертого класса использовать всю доступную пропускную способность.	[edit] admin@edge# set policy qos shaper Shaper-VPN-Output class 4 ceiling 100%
Определение алгоритма справедливой очереди для трафика четвертого класса.	[edit] admin@edge# set policy qos shaper Shaper-VPN-Output class 4 queue-type fair-queue
Установка значения лимита пакетов в очереди для трафика четвертого класса.	[edit] admin@edge# set policy qos shaper Shaper-VPN-Output class 4 queue-limit 127
Создание фильтра с правилом определения TCP-	[edit]

Действие	**Команда**
трафика	`admin@edge# set filter TCP-traffic rule 10 protocol tcp`
Фиксация изменения.	`[edit]` `admin@edge# commit`

Вывод настроек фильтра для определения TCP-трафика.	`[edit]`
	`admin@edge# show filter TCP-traffic`
	`rule 10 {`
	`protocol tcp`
	`}`

Определение соответствия трафика четвертого класса на основе фильтра TCP-traffic.	`[edit]` `admin@edge# set policy qos shaper Shaper-VPN-Output class 4 match TCP-traffic filter TCP-traffic`
Определение алгоритма очереди для трафика VPN-туннеля согласно определённой дочерней политике Shaper-VPN-Output.	`[edit]` `admin@edge# set policy qos shaper Shaper-Output class 2 queue-ref Shaper-VPN-Output`
Создание узла конфигурации для политики QoS.	`[edit]` `admin@edge# set policy qos shaper Shaper-Internet-Output`
Добавление описания.	`[edit]` `admin@edge# set policy qos shaper Shaper-Internet-Output description "Output shaper Internet traffic"`
Установка суммарной пропускной способности канала.	`[edit]` `admin@edge# set policy qos shaper Shaper-Internet-Output bandwidth auto`
Назначение пропускной способности для трафика по умолчанию.	`[edit]` `admin@edge# set policy qos shaper Shaper-Internet-Output default bandwidth 93%`
Разрешение трафику по умолчанию использовать всю доступную пропускную способность.	`[edit]` `admin@edge# set policy qos shaper Shaper-Internet-Output default ceiling 100%`
Добавление описания для трафика второго класса – SMTP-трафика.	`[edit]` `admin@edge# set policy qos shaper Shaper-Internet-Output class 2 description "SMTP-traffic"`
Назначение пропускной способности для трафика второго класса.	`[edit]` `admin@edge# set policy qos shaper Shaper-Internet-Output class 2 bandwidth 7%`
Разрешение трафику второтго класса использовать всю доступную пропускную способность.	`[edit]` `admin@edge# set policy qos shaper Shaper-Internet-Output class 2 ceiling 100%`
Определение алгоритма с отбрасыванием конца очереди для трафика второго класса.	`[edit]` `admin@edge# set policy qos shaper Shaper-Internet-Output class 2 queue-type drop-tail`
Создание фильтра с правилом определения SMTP-трафика (по протоколам TCP и UDP).	`[edit]` `admin@edge# set filter SMTP-traffic rule 10 protocol tcp_udp`
Добавление к фильтру правила определения исходящего SMTP-трафика на порт 25.	`[edit]` `admin@edge# set filter SMTP-traffic rule 10 source port 25`
Создание фильтра с правилом определения SMTP-трафика (по протоколам TCP и UDP).	`[edit]` `admin@edge# set filter SMTP-traffic rule 20 protocol tcp_udp`
Добавление к фильтру правила определения входящего SMTP-трафика на порт 25.	`[edit]` `admin@edge# set filter SMTP-traffic rule`

Действие	Команда
	20 destination port 25
Фиксация изменения.	[edit] admin@edge# commit

Вывод настроек фильтра для определения SMTP-трафика.	[edit]
	admin@edge# show filter SMTP-traffic
	rule 10 {
	protocol tcp_udp
	source {
	port 25
	}
	}
	rule 20 {
	protocol tcp_udp
	destination {
	port 25
	}
	}

Определение соответствия трафика второго класса на основе фильтра SMTP-traffic.	[edit] admin@edge# set policy qos shaper Shaper-Internet-Output class 10 match SMTP-traffic filter SMTP-traffic
Определение алгоритма очереди для Интернет трафика согласно определённой дочерней политике Shaper-Internet-Output.	[edit] admin@edge# set policy qos shaper Shaper-Output default queue-ref Shaper-Internet-Output
Фиксация изменения.	[edit] admin@edge# commit

Вывод настройки policy qos.	[edit]
	admin@edge# show policy qos
	shaper Shaper-Internet-Output {
	bandwidth auto
	class 2 {
	bandwidth 7%
	ceiling 100%
	description SMTP-traffic
	match SMTP-traffic {
	filter SMTP-traffic
	}
	queue-type drop-tail
	}
	default {
	bandwidth 93%
	ceiling 100%
	}
	description "Output shaper Internet traffic"
	}
	shaper Shaper-Output {
	bandwidth 10mbit
	class 2 {
	bandwidth 40%
	ceiling 100%
	description "VPN segment"
	match VPN-traffic {
	filter VPN-traffic
	}
	queue-ref Shaper-VPN-Output
	}
	default {
	bandwidth 60%
	ceiling 100%

Действие	Команда

	queue-ref Shaper-Internet-Output
	}
	description "Output shaper VPN and Internet traffic"
	}
	shaper Shaper-VPN-Output {
	bandwidth auto
	class 2 {
	bandwidth 5%
	ceiling 100%
	description "SIP traffic"
	match SIP-traffic {
	filter SIP-traffic
	}
	queue-type drop-tail
	}
	class 3 {
	bandwidth 25%
	ceiling 100%
	description RTP-traffic
	match RTP-traffic {
	filter RTP-traffic
	}
	queue-type drop-tail
	}
	class 4 {
	bandwidth 60%
	ceiling 100%
	description TCP-traffic
	match TCP-traffic {
	filter TCP-traffic
	}
	queue-limit 127
	queue-type fair-queue
	}
	default {
	bandwidth 10%
	ceiling 100%
	}
	description "Output shaper SIP-RTP-TCP traffic"
	}

Назначение политики QoS интерфейсу, через который осуществляется подключение к Интернет-провайдеру.	[edit] admin@edge# set interfaces ethernet eth0 policy out qos Shaper-Output
Фиксация изменения.	[edit] admin@edge# commit

Вывод перечня политик QoS назначенных, интерфейсу, через который осуществляется подключение к Интернет-провайдеру.	[edit]
	admin@edge# show interfaces ethernet eth0 policy
	out {
	qos Shaper-Output
	}

22.2 Команды QoS

В данном разделе описаны команды для функций QoS, поддерживаемых Numa Edge.

В данном разделе приведены следующие команды.

Таблица 178 – описаны команды для функций QoS

Команды настройки	
Применение политик QoS к интерфейсам	
interfaces <интерфейс> policy <направление> qos <имя_политики>	Применение политики QoS к указанному интерфейсу.
Политики отбрасывания конца очереди	
policy qos drop-tail <имя_политики>	Определение политики QoS с отбрасыванием конца очереди (чистая дисциплина FIFO).
policy qos drop-tail <имя_политики> description <описание>	Указание текстового описания для политики QoS с отбрасыванием конца очереди.
policy qos drop-tail <имя_политики> queue-limit <ограничение>	Установка верхней границы разрешенного числа пакетов в очереди для политики отбрасывания конца очереди.
Политики справедливой очереди	
policy qos fair-queue <имя_политики>	Определение политики QoS со справедливой очередью.
policy qos fair-queue <имя_политики> description <описание>	Указание текстового описания для политики справедливой очереди.
policy qos fair-queue <имя_политики> hash-interval <секунды>	Указание интервала между обновлениями функции хеширования потока для политики справедливой очереди.
policy qos fair-queue <имя_политики> queue-limit <ограничение>	Установка верхней границы разрешенного числа пакетов в очереди для политики справедливой очереди.
Политики имитации сети	
policy qos network-emulator <имя_политики>	Определение политики QoS с имитацией сети.
policy qos network-emulator <имя_политики> bandwidth <скорость>	Указание ограничения пропускной способности для всего суммарного трафика, ограничиваемого данной политикой.
policy qos network-emulator <имя_политики> burst <размер>	Установка размера непрерывной серии пакетов для политики QoS с имитацией сети.
policy qos network-emulator <имя_политики> description <описание>	Указание текстового описания для политики имитации сети.
policy qos network-emulator <имя_политики> network-delay <задержка>	Установка величины задержки между пакетами для политики QoS с имитацией сети.
policy qos network-emulator <имя_политики> packet-corruption <процент>	Установка процентной доли пакетов, подлежащих повреждению, в политике QoS с имитацией сети.
policy qos network-emulator <имя_политики> packet-loss <процент>	Установка процентной доли пакетов, подлежащих потере, в политике QoS с имитацией сети.
policy qos network-emulator <имя_политики> packet-reordering <процент>	Установка процентной доли пакетов, подлежащих изменению порядка следования, в политике QoS с имитацией сети.
policy qos network-emulator <имя_политики> queue-limit <ограничение>	Установка верхней границы разрешенного числа пакетов в очереди для политики QoS с имитацией сети.
Политики приоритизированной очереди	
policy qos priority-queue <имя_политики>	Определение политики QoS с приоритизированной очередью.
policy qos priority-queue <имя_политики> description <описание>	Указание текстового описания для политики QoS с приоритизированной очередью
Классы для политики приоритизированной очереди	
policy qos priority-queue <имя_политики> class <класс>	Определение класса трафика для политики QoS с приоритизированной очередью.
policy qos priority-queue <имя_политики> class <класс> description <описание>	Указание текстового описания для класса трафика.

policy qos priority-queue <имя_политики> class <класс> match <имя_правила>	Определение правила для проверки соответствия классов трафика.
policy qos priority-queue <имя_политики> class <класс> match <имя_правила> description <описание>	Указание текстового описания для правила соответствия.
policy qos priority-queue <имя_политики> class <класс> match <имя_правила> ether destination <mac_адрес>	Указание критерия соответствия на основе MAC-адреса получателя.
policy qos priority-queue <имя_политики> class <класс> match <имя_правила> ether protocol <тип_кадра>	Указание критерия соответствия на основе типа пакета Ethernet.
policy qos priority-queue <имя_политики> class <класс> match <имя_правила> ether source <mac_адрес>	Указание критерия соответствия на основе MAC-адреса отправителя.
policy qos priority-queue <имя_политики> class <класс> match <имя_правила> interface <интерфейс>	Указание критерия соответствия на основе входного интерфейса пакетов.
policy qos priority-queue <имя_политики> class <класс> match <имя_правила> filter <имя_фильтра>	Указание критерия соответствия на основе определённого фильтра IPv4-трафика.
policy qos priority-queue <имя_политики> class _<класс> match <имя_правила> filter-ipv6 <имя_фильтра>	Указание критерия соответствия на основе определённого фильтра IPv6-трафика.
policy qos priority-queue <имя_политики> class <класс> match <имя_правила> vif <идентификатор_vlan>	Указание критерия соответствия на основе идентификатора VLAN.
policy qos priority-queue <имя_политики> class <класс> queue-limit <ограничение>	Указание максимального размера очереди для класса трафика.
policy qos priority-queue <имя_политики> class <класс> queue-ref <имя_политики>	Указание дочерней политики QoS для данного класса трафика.
policy qos priority-queue <имя_политики> class <класс> queue-type <тип>	Указание типа работы с очередью, используемого для класса трафика.
policy qos priority-queue <имя_политики> default	Определение политики QoS по умолчанию с приоритизированной очередью.
policy qos priority-queue <имя_политики> default queue-limit <ограничение>	Указание максимального размера очереди для класса трафика по умолчанию.
policy qos priority-queue <имя_политики> default queue-ref <имя_политики>	Указание дочерней политики QoS по умолчанию.
policy qos priority-queue <имя_политики> default queue-type <тип>	Указание типа работы с очередью, используемого для класса трафика по умолчанию.
Политики случайного определения	
policy qos random-detect <имя_политики>	Определение политики QoS со взвешенным случайным ранним определением (WRED).
policy qos random-detect <имя_политики> bandwidth <скорость>	Указание ограничения пропускной способности для всего суммарного трафика, ограничиваемого данной политикой.
policy qos random-detect <имя_политики> description <описание>	Указание текстового описания для политики случайного определения.
policy qos random-detect <имя_политики> precedence <предпочтительность>	Установка параметров отбрасывания пакетов на основе предпочтительности для политики случайного определения.
Политики ограничения скорости	
policy qos rate-control <имя_политики>	Определение политики QoS с ограничением скорости.

policy qos rate-control <имя_политики> bandwidth <скорость>	Указание ограничения пропускной способности для всего суммарного трафика, ограничиваемого данной политикой.
policy qos rate-control <имя_политики> burst <размер>	Установка размера непрерывной серии пакетов для политики QoS с ограничением скорости.
policy qos rate-control <имя_политики> description <описание>	Указание текстового описания для политики ограничения скорости.
policy qos rate-control <имя_политики> latency <задержка>	Установка ограничения на размер очереди на основе задержки для политики QoS с ограничением скорости.
Политики циклического перебора	
policy qos round-robin <имя_политики>	Определение политики QoS с циклическим перебором.
policy qos round-robin <имя_политики> description <описание>	Указание текстового описания для политики QoS с циклическим перебором.
Классы для политики циклического перебора	
policy qos round-robin <имя_политики> class <класс>	Определение класса трафика для политики QoS с циклическим перебором.
policy qos round-robin <имя_политики> class <класс> description <описание>	Указание текстового описания для класса трафика.
policy qos round-robin <имя_политики> class <класс> match <имя_правила>	Определение правила для проверки соответствия классов трафика.
policy qos round-robin <имя_политики> class <класс> match <имя_правила> description <описание>	Указание текстового описания для правила соответствия.
policy qos round-robin <имя_политики> class <класс> match <имя_правила> ether destination <mac_адрес>	Указание критерия соответствия на основе MAC-адреса получателя.
policy qos round-robin <имя_политики> class <класс> match <имя_правила> ether protocol <тип_кадра>	Указание критерия соответствия на основе типа пакета Ethernet.
policy qos round-robin <имя_политики> class <класс> match <имя_правила> ether source <mac_адрес>	Указание критерия соответствия на основе MAC-адреса отправителя.
policy qos round-robin <имя_политики> class <класс> match <имя_правила> interface <интерфейс>	Указание критерия соответствия на основе входного интерфейса пакетов.
policy qos round-robin <имя_политики> class <класс> match <имя_правила> filter <имя_фильтра>	Указание критерия соответствия на основе определённого фильтра IPv4-трафика.
policy qos round-robin <имя_политики> class <класс> match <имя_правила> filter-ipv6 <имя_фильтра>	Указание критерия соответствия на основе определённого фильтра IPv6-трафика.
policy qos round-robin <имя_политики> class <класс> match <имя_правила> vif <идентификатор_vlan>	Указание критерия соответствия на основе идентификатора VLAN.
policy qos round-robin <имя_политики> class <класс> quantum <число_пакетов>	Указание числа пакетов, которые могут быть отправлены за квант планирования.
policy qos round-robin <имя_политики> class <класс> queue-limit <ограничение>	Указание максимального размера очереди для класса трафика.
policy qos round-robin <имя_политики> class <класс> queue-ref <имя_политики>	Указание дочерней политики QoS для данного класса трафика.
policy qos round-robin <имя_политики> class <класс> queue-type <тип>	Указание типа работы с очередью, используемого для класса трафика.
Класс по умолчанию для политики циклического перебора	
policy qos round-robin <имя_политики> default	Определение политики QoS по умолчанию с циклическим перебором.
policy qos round-robin <имя_политики> default quantum <число_пакетов>	Указание числа пакетов, которые могут быть отправлены за квант планирования.
policy qos round-robin <имя_политики> default queue-limit <ограничение>	Указание максимального размера очереди для класса трафика по умолчанию.
policy qos round-robin <имя_политики> default queue-ref <имя_политики>	Указание дочерней политики QoS по умолчанию.

policy qos round-robin <имя_политики> default queue-type <тип>	Указание типа работы с очередью, используемого для класса трафика по умолчанию.
Политики ограничения трафика	
policy qos limiter <имя_политики>	Определение политики QoS с ограничением трафика.
policy qos limiter <имя_политики> description <описание>	Указание текстового описания политики QoS с ограничением трафика.
Классы для политики ограничения трафика	
policy qos limiter <имя_политики> class <класс>	Определение класса трафика для политики QoS с ограничением трафика.
policy qos limiter <имя_политики> class <класс> bandwidth <скорость>	Указание ограничения пропускной способности для класса трафика.
policy qos limiter <имя_политики> class <класс> burst <размер>	Установка размера непрерывной серии пакетов для класса трафика.
policy qos limiter <имя_политики> class <класс> description <описание>	Указание текстового описания для класса трафика.
policy qos limiter <имя_политики> class <класс> match <имя_правила>	Определение правила для проверки соответствия классов трафика.
policy qos limiter <имя_политики> class <класс> match <имя_правила> description <описание>	Указание текстового описания для правила соответствия.
policy qos limiter <имя_политики> class <класс> match <имя_правила> ether destination <mac_адрес>	Указание критерия соответствия на основе MAC-адреса получателя.
policy qos limiter <имя_политики> class <класс> match <имя_правила> ether protocol <тип_кадра>	Указание критерия соответствия на основе типа пакета Ethernet.
policy qos limiter <имя_политики> class <класс> match <имя_правила> ether source <mac_адрес>	Указание критерия соответствия на основе MAC-адреса отправителя.
policy qos limiter <имя_политики> class <класс> match <имя_правила> ip destination	Указание критерия соответствия на основе сведений IP о получателе.
policy qos limiter <имя_политики> class <класс> match <имя_правила> ip dscp <значение>	Указание критерия соответствия на основе значения поля DSCP.
policy qos limiter<имя_политики> class <класс> match <имя_правила> ip protocol <протокол>	Указание критерия соответствия на основе протокола IP.
policy qos limiter <имя_политики> class <класс> match <имя_правила> ip source	Указание критерия соответствия на основе сведений IP об отправителе.
policy qos limiter <имя_политики> class <класс> match <имя_правила> ipv6 destination	Указание критерия соответствия на основе сведений IPv6 о получателе.
policy qos limiter <имя_политики> class <класс> match <имя_правила> ipv6 dscp <значение>	Указание критерия соответствия на основе значения поля DSCP.
policy qos limiter <имя_политики> class <класс> match <имя_правила> ipv6 protocol <протокол>	Указание критерия соответствия на основе протокола IPv6.
policy qos limiter <имя_политики> class <класс> match <имя_правила> ipv6 source	Указание критерия соответствия на основе сведений IPv6 об отправителе.
policy qos limiter <имя_политики> class <класс> match <имя_правила> vif <идентификатор_vlan>	Указание критерия соответствия на основе идентификатора VLAN.
policy qos limiter <имя_политики> class <класс> priority <приоритет>	Указания порядка обработки правил соответствия.
Политики управления загрузкой канала	
policy qos shaper <имя_политики>	Определение политики QoS с управлением загрузкой канала.
policy qos shaper <имя_политики> bandwidth <скорость>	Указание пропускной способности, доступной для всего суммарного трафика, ограничиваемого данной политикой.
policy qos shaper <имя_политики> description <описание>	Указание текстового описания для политики QoS с управлением загрузкой канала.

Классы для политики управления загрузкой канала	
policy qos shaper <имя_политики> class <класс>	Определение класса трафика для политики QoS с управлением загрузкой канала.
policy qos shaper <имя_политики> class <класс> bandwidth <скорость>	Указание базовой гарантированной пропускной способности для класса трафика.
policy qos shaper <имя_политики> class <класс> burst <размер>	Установка размера непрерывной серии пакетов для класса трафика.
policy qos shaper <имя_политики> default ceiling <скорость>	Установка верхней границы пропускной способности для класса трафика.
policy qos shaper <имя_политики> class <класс> description <описание>	Указание текстового описания для класса трафика.
policy qos shaper <имя_политики> class <класс> match <имя_правила>	Определение правила для проверки соответствия классов трафика.
policy qos shaper <имя_политики> class <класс> match <имя_правила> description <описание>	Указание текстового описания для правила соответствия.
policy qos shaper <имя_политики> class <класс> match <имя_правила> ether destination <mac_адрес>	Указание критерия соответствия на основе MAC-адреса получателя.
policy qos shaper <имя_политики> class <класс> match <имя_правила> ether protocol <тип_кадра>	Указание критерия соответствия на основе типа пакета Ethernet.
policy qos shaper <имя_политики> class <класс> match <имя_правила> ether source <mac_адрес>	Указание критерия соответствия на основе MAC-адреса отправителя.
policy qos shaper <имя_политики> class <класс> match <имя_правила> filter <имя_фильтра>	Указание критерия соответствия на основе определённого фильтра IPv4-трафика.
policy qos shaper <имя_политики> class <класс> match <имя_правила> filter-ipv6 <имя_фильтра>	Указание критерия соответствия на основе определённого фильтра IPv6-трафика.
policy qos shaper <имя_политики> class <класс> match <имя_правила> interface <интерфейс>	Указание критерия соответствия на основе входного интерфейса пакетов.
policy qos shaper <имя_политики> class <класс> match <имя_правила> vif <идентификатор_vlan>	Указание критерия соответствия на основе идентификатора VLAN.
policy qos shaper <имя_политики> class <класс> priority <приоритет>	Указание приоритета класса трафика при выделении дополнительной пропускной способности.
policy qos shaper <имя_политики> class <класс> queue-limit <ограничение>	Указание максимального размера очереди для класса трафика.
policy qos shaper <имя_политики> class <класс> queue-ref <имя_политики>	Указание дочерней политики QoS для данного класса трафика.
policy qos shaper <имя_политики> class <класс> queue-type <тип>	Указание типа работы с очередью, используемого для класса трафика.
Класс по умолчанию для политики управления загрузкой канала	
policy qos shaper <имя_политики> default	Определение политики QoS по умолчанию с управлением загрузкой канала.
policy qos shaper <имя_политики> default bandwidth <скорость>	Указание базовой гарантированной пропускной способности для класса трафика по умолчанию.
policy qos shaper <имя_политики> **default** burst	Установка размера непрерывной серии пакетов для класса трафика по умолчанию.
policy qos shaper <имя_политики> default ceiling <скорость>	Установка верхней границы пропускной способности для класса трафика по умолчанию.
policy qos shaper <имя_политики> default priority <приоритет>	Указание приоритета класса трафика по умолчанию при выделении дополнительной пропускной способности.
policy qos shaper <имя_политики> default queue-limit <ограничение>	Указание максимального размера очереди для класса трафика по умолчанию.
policy qos shaper <имя_политики> default queue-ref <имя_политики>	Указание дочерней политики QoS по умолчанию.

policy qos shaper <имя_политики> default queue-type <тип>	Указание типа работы с очередью, используемого для класса трафика по умолчанию.
Эксплуатационные команды	
show incoming	Отображение входящих политик QoS.
show queueing	Отображение текущих политик QoS.

22.2.1 interfaces <интерфейс> policy <направление> qos <имя_политики>

Применение политики QoS к указанному интерфейсу.

Синтаксис

```
set interfaces <тип_интерфейса> <интерфейс> policy <направление> qos <имя_политики>

delete interfaces <тип_интерфейса> <интерфейс> policy <направление> qos

show interfaces <тип_интерфейса> <интерфейс> policy <направление> qos
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
    policy {
        направление {
            qos имя_политики
        }
    }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже в разделе Указания по использованию.

направление

Обязательный. Направление трафика, к которому применяется политика QoS. Допустимые значения указаны в таблице ниже:

Таблица 179 – Направления трафика

Значение	Описание
in	Транзитный трафик, принимаемый на указанном интерфейсе
out	Транзитный трафик, отправляемый с указанного интерфейса

имя_политики

Имя политики QoS, применяемой к данному интерфейсу.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для применения политики QoS к интерфейсу.

На каждом интерфейсе можно применить до двух политик QoS: одну для транзитного трафика, принимаемого на интерфейсе (in), одну – для транзитного трафика, покидающего интерфейс (out).

В приведенной ниже таблице показаны типы поддерживаемых интерфейсов и синтаксис.

Таблица 180 – Типы интерфейсов

Тип интерфейса	Синтаксис
Агрегирование каналов	bonding bondx
Виртуальный интерфейс агрегированных каналов	bonding bondx vif идентификатор_vlan
Сетевой мост	bridge brx
Ethernet	ethernet ethx
Ethernet PPPoE	ethernet ethx pppoe номер
Виртуальный интерфейс Ethernet	ethernet ethx vif идентификатор_vlan
Ethernet Vif PPPoE	ethernet ethx vif идентификатор_vlan pppoe номер
Интерфейс заглушки	loopback lo
Многоканальная связь	multilink mlx
OpenVPN	openvpn vtunx
Псевдо-Ethernet	pseudo-ethernet pethx
Последовательный интерфейс	serial srx vif идентификатор_vlan
Туннель	tunnel tunx

Форма **set** этой команды используется для применения политики QoS к интерфейсу.

Форма **delete** этой команды используется для удаления политики QoS с интерфейса.

Форма **show** этой команды используется для отображения настройки политики QoS на интерфейсе.

22.2.2 policy qos drop-tail <имя_политики>

Определение политики QoS с отбрасыванием конца очереди (чистая дисциплина FIFO).

Синтаксис

```
set policy qos drop-tail <имя_политики>
delete policy qos drop-tail <имя_политики>
show policy qos drop-tail <имя_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      drop-tail имя_политики {
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики отбрасывания конца очереди.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения политики QoS с отбрасыванием конца очереди. Политика отбрасывания конца очереди применима только к исходящему трафику. Имя политики должно быть уникальным и еще не использованным в других командах политик QoS.

Политика отбрасывания конца очереди предоставляет механизм работы с очередями по дисциплине FIFO (первым пришел - первым ушел).

Форма **set** этой команды используется для создания политики отбрасывания конца очереди.

Форма **delete** этой команды используется для удаления политики отбрасывания конца очереди.

Форма **show** этой команды используется для отображения настройки политики отбрасывания конца очереди.

22.2.3 policy qos drop-tail <имя_политики> description <описание>

Указание текстового описания для политики QoS с отбрасыванием конца очереди.

Синтаксис

```
set policy qos drop-tail <имя_политики> description <описание>
delete policy qos drop-tail <имя_политики> description
show policy qos drop-tail <имя_политики> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      drop-tail имя_политики {
         description описание
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики отбрасывания конца очереди.

описание

Необязательный. Описание для данной политики отбрасывания конца очереди.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для записи описания политики отбрасывания конца очереди.

Форма **set** этой команды используется для указания описания.

Форма **delete** этой команды используется для удаления описания.

Форма **show** этой команды используется для отображения настройки описания.

22.2.4 policy qos drop-tail <имя_политики> queue-limit <ограничение>

Установка верхней границы разрешенного числа пакетов в очереди для политики отбрасывания конца очереди.

Синтаксис

```
set policy qos drop-tail <имя_политики> queue-limit <ограничение>
delete policy qos drop-tail <имя_политики> queue-limit
show policy qos drop-tail <имя_политики> queue-limit
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      drop-tail имя_политики {
         queue-limit ограничение
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики отбрасывания конца очереди.

ограничение

Необязательный. Максимальный размер очереди в пакетах.

Значение по умолчанию

Для Ethernet длина очереди, равна 1000 пакетов.

Указания по использованию

Эта команда используется для установки максимального числа пакетов, которые могут стоять в очереди, при использовании данной политики работы с очередями. Если достигнута максимальная длина очереди, система начинает отбрасывать пакеты.

Форма **set** этой команды используется для установки ограничения длины очереди.

Форма **delete** этой команды используется для восстановления длины очереди по умолчанию.

Форма **show** этой команды используется для отображения настройки ограничения длины очереди.

22.2.5 policy qos fair-queue <имя_политики>

Определение политики QoS со справедливой очередью.

Синтаксис

```
set policy qos fair-queue <имя_политики>
delete policy qos fair-queue <имя_политики>
show policy qos fair-queue <имя_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      fair-queue имя_политики {
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики справедливой очереди.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения политики QoS со справедливой очередью (FQ). Политика FQ применима только к исходящему трафику. Имя политики должно быть уникальным и еще не использованным в других командах политик QoS.

В Numa Edge используется алгоритм SFQ, один из алгоритмов FQ, целью которого является обеспечение справедливого доступа на уровне потоков. Алгоритм FQ пытается обеспечить справедливый доступ к сетевым ресурсам и предотвратить захват одним потоком чрезмерной доли пропускной способности выходного порта.

В алгоритме SFQ пропускная способность делится на раздельные индексные сегменты на основании сочетания протокола IP и адресов отправителя и получателя таким образом, чтобы ни один поток не получил несправедливой порции пропускной способности.

Форма **set** этой команды используется для создания политики справедливой очереди.

Форма **delete** этой команды используется для удаления политики справедливой очереди.

Форма **show** этой команды используется для отображения настройки политики справедливой очереди.

22.2.6 policy qos fair-queue <имя_политики> description <описание>

Указание текстового описания для политики справедливой очереди.

Синтаксис

```
set policy qos fair-queue <имя_политики> description <описание>
delete policy qos fair-queue <имя_политики> description
show policy qos fair-queue <имя_политики> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      fair-queue имя_политики {
         description описание
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики справедливой очереди.

описание

Необязательный. Описание для данной политики справедливой очереди.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для записи описания политики справедливой очереди.

Форма **set** этой команды используется для указания описания.

Форма **delete** этой команды используется для удаления описания.

Форма **show** этой команды используется для отображения настройки описания.

22.2.7 policy qos fair-queue <имя_политики> hash-interval <секунды>

Указание интервала между обновлениями функции хеширования потока для политики справедливой очереди.

Синтаксис

```
set policy qos fair-queue <имя_политики> hash-interval <секунды>
delete policy qos fair-queue <имя_политики> hash-interval
show policy qos fair-queue <имя_политики> hash-interval
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      fair-queue имя_политики {
         hash-interval секунды
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики справедливой очереди.

секунды

Необязательный. Интервал повторного вычисления функции контрольной суммы (хеширования) в секундах. 0 означает, что функция хеширования никогда не обновляется.

Значение по умолчанию

Функция хеширования никогда не обновляется.

Указания по использованию

Эта команда используется для установки интервала обновления функции хеширования потока.

Регулярное обновление функции хеширования увеличивает безопасность и предотвращает атаки на основе определения индексного сегмента злоумышленником и последующей отправки пакетов, подмененных на основе полученных данных.

Форма **set** этой команды используется для указания интервала обновления функции хеширования потока.

Форма **delete** этой команды используется для восстановления интервала хеширования по умолчанию.

Форма **show** этой команды используется для отображения настройки интервала хеширования.

22.2.8 policy qos fair-queue <имя_политики> queue-limit <ограничение>

Установка верхней границы разрешенного числа пакетов в очереди для политики справедливой очереди.

Синтаксис

```
set policy qos fair-queue <имя_политики> queue-limit <ограничение>
delete policy qos fair-queue <имя_политики> queue-limit
show policy qos fair-queue <имя_политики> queue-limit
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      fair-queue имя_политики {
         queue-limit ограничение
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики справедливой очереди.

ограничение

Необязательный. Максимальный размер очереди в пакетах. Значение должно находиться в диапазоне от 2 до 127.

Значение по умолчанию

Длина очереди не должна превосходить 127 пакетов.

Указания по использованию

Эта команда используется для установки максимального числа пакетов, которые могут стоять в очереди, при использовании данной политики работы с очередями. Если достигнута максимальная длина очереди, система начинает отбрасывать пакеты.

Форма **set** этой команды используется для установки ограничения длины очереди.

Форма **delete** этой команды используется для восстановления длины очереди по умолчанию.

Форма **show** этой команды используется для отображения настройки ограничения длины очереди.

22.2.9 policy qos network-emulator <имя_политики>

Определение политики QoS с имитацией сети.

Синтаксис

```
set policy qos network-emulator <имя_политики>
delete policy qos network-emulator <имя_политики>
show policy qos network-emulator <имя_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      network-emulator имя_политики {
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики имитации сети.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения политики QoS, используемой при имитации сетей ГВС. Имя политики должно быть уникальным и еще не использованным в других командах политик QoS.

Форма **set** этой команды используется для создания политики QoS с имитацией сети.

Форма **delete** этой команды используется для удаления политики QoS с имитацией сети.

Форма **show** этой команды используется для отображения настройки политики QoS с имитацией сети.

22.2.10 policy qos network-emulator <имя_политики> bandwidth <скорость>

Указание ограничения пропускной способности для всего суммарного трафика, ограничиваемого данной политикой.

Синтаксис

```
set policy qos network-emulator <имя_политики> bandwidth <скорость>
delete policy qos network-emulator <имя_политики> bandwidth
show policy qos network-emulator <имя_политики> bandwidth
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      network-emulator имя_политики {
         bandwidth скорость
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики имитации сети.

скорость

Необязательный. Пропускная способность. Допустимые форматы представлены в таблице ниже.

Таблица 181 – Формат указания пропускной способности

Значение	Описание
<число>	Пропускная способность указанная в килобайтах в секунду.
<число><приставка>	Пропускная способность в указанных единицах измерения. Поддерживаются следующие единицы измерения: **kbit:** килобит в секунду. **mbit:** мегабит в секунду. **gbit:** гигабит в секунду. **kbps:** килобайт в секунду. **mbps:** мегабайт в секунду. **gbps:** гигабайт в секунду.

Значение по умолчанию

Трафик передается на максимальной скорости.

Указания по использованию

Эта команда используется для установки ограничений пропускной способности в политике QoS с имитацией сети. Определяется максимальная пропускная способность, доступная политике имитации сети.

Форма **set** этой команды используется для указания ограничений пропускной способности для политики.

Форма **delete** этой команды используется для восстановления ограничений пропускной способности по умолчанию.

Форма **show** этой команды используется для отображения настройки пропускной способности, выделенной политике.

22.2.11 policy qos network-emulator <имя_политики> burst <размер>

Установка размера непрерывной серии пакетов для политики QoS с имитацией сети.

Синтаксис

```
set policy qos network-emulator <имя_политики> burst <размер>
delete policy qos network-emulator <имя_политики> burst
show policy qos network-emulator <имя_политики> burst
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      network-emulator имя_политики {
         burst размер
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики имитации сети.

размер

Необязательный. Размер непрерывной серии. Размер непрерывной серии должен находиться в промежутке между 15 КБ и 32 МБ. Допустимые форматы представлены в таблице ниже.

Таблица 182 – Формат указания размера непрерывной серии.

Значение	Описание
<число>	Размер непрерывной серии указанный в байтах.
<число><приставка>	Размер непрерывной серии в указанных единицах измерения. Поддерживаются следующие единицы измерения: **kb:** килобайты. **mb:** мегабайты.

Значение по умолчанию

Длина непрерывной серии по умолчанию 15 килобайт.

Указания по использованию

Эта команда используется для установки размера непрерывной серии пакетов в политике QoS с имитацией сети. Устанавливается максимальный объем трафика, который может быть передан за один раз; параметр используется только вместе с параметром пропускной способности.

Форма **set** этой команды используется для указания размера непрерывной серии пакетов в политике QoS с имитацией сети.

Форма **delete** этой команды используется для восстановления размера непрерывной серии по умолчанию в политике QoS с имитацией сети.

Форма **show** этой команды используется для отображения настройки размера непрерывной серии в политике имитации сети.

22.2.12 policy qos network-emulator <имя_политики> description <описание>

Указание текстового описания для политики имитации сети.

Синтаксис

```
set policy qos network-emulator <имя_политики> description <описание>
delete policy qos network-emulator <имя_политики> description
show policy qos network-emulator <имя_политики> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      network-emulator имя_политики {
         description описание
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики имитации сети.

описание

Необязательный. Описание для данной политики имитации сети.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для записи описания политики имитации сети.

Форма **set** этой команды используется для указания описания.

Форма **delete** этой команды используется для удаления описания.

Форма **show** этой команды используется для отображения настройки описания.

22.2.13 policy qos network-emulator <имя_политики> network-delay <задержка>

Установка величины задержки между пакетами для политики QoS с имитацией сети.

Синтаксис

```
set policy qos network-emulator <имя_политики> network-delay <задержка>
delete policy qos network-emulator <имя_политики> network-delay
show policy qos network-emulator <имя_политики> network-delay
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      network-emulator имя_политики {
         network-delay задержка
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики имитации сети.

задержка

Задержка между пакетами. Допустимые форматы:

Таблица 183 – Формат указания задержки между пакетами.

Значение	Описание
<число>	Задержка между пакетами в секундах.
<число><приставка>	Задержка между пакетами в указанных единицах измерения. Поддерживаются следующие единицы измерения: **secs:** секунды. **ms:** миллисекунды. **us:** микросекунды.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки задержки сети в политике QoS с имитацией сети. Указывается задержка, которую следует добавить между пакетами.

Форма **set** этой команды используется для указания задержки сети в политике QoS с имитацией сети.

Форма **delete** этой политики используется для восстановления задержки сети по умолчанию в политике QoS с имитацией сети.

Форма **show** этой команды используется для отображения настройки задержки сети.

22.2.14 policy qos network-emulator <имя_политики> packet-corruption <процент>

Установка процентной доли пакетов, подлежащих повреждению, в политике QoS с имитацией сети.

Синтаксис

```
set policy qos network-emulator <имя_политики> packet-corruption <процент>
delete policy qos network-emulator <имя_политики> packet-corruption
show policy qos network-emulator <имя_политики> packet-corruption
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      network-emulator имя_политики {
         packet-corruption процент
```

```
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики имитации сети.

процент

Процентная доля пакетов, подлежащих случайному повреждению. Значение должно находится в диапазоне от 0 до 100.

Значение по умолчанию

Пакеты не повреждаются (т.е. 0%).

Указания по использованию

Эта команда используется для установки процентной доли пакетов, подлежащих повреждению, в политике QoS с имитацией сети. Повреждение такого рода имитирует неисправности канала, вызывающие повреждение пакетов, путем обращения одного случайного бита в пакете без изменения контрольной суммы.

Форма **set** этой команды используется для указания процентной доли пакетов, подлежащих случайному повреждению, в политике QoS с имитацией сети.

Форма **delete** этой команды используется для восстановления процентной доли по умолчанию пакетов, подлежащих повреждению, в политике QoS с имитацией сети.

Форма **show** этой команды используется для отображения настройки повреждения пакетов.

22.2.15 policy qos network-emulator <имя_политики> packet-loss <процент>

Установка процентной доли пакетов, подлежащих потере, в политике QoS с имитацией сети.

Синтаксис

```
set policy qos network-emulator <имя_политики> packet-loss <процент>
delete policy qos network-emulator <имя_политики> packet-loss
show policy qos network-emulator <имя_политики> packet-loss
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        network-emulator имя_политики {
            packet-loss процент
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики имитации сети.

процент

Процентная доля пакетов, подлежащих случайному отбрасыванию. Значение должно находится в диапазоне от 0 до 100.

Значение по умолчанию

Пакеты не отбрасываются (т.е. 0%).

Указания по использованию

Эта команда используется для установки процентной доли пакетов, подлежащих отбрасыванию, в политике QoS с имитацией сети. Отбрасывание такого рода имитирует неисправности канала, вызывающие потерю пакетов.

Форма **set** этой команды используется для указания процентной доли пакетов, подлежащих случайному отбрасыванию, в политике QoS с имитацией сети.

Форма **delete** этой команды используется для восстановления процентной доли по умолчанию пакетов, подлежащих отбрасыванию, в политике QoS с имитацией сети.

Форма **show** этой команды используется для отображения настройки потери пакетов.

22.2.16 policy qos network-emulator <имя_политики> packet-reordering <процент>

Установка процентной доли пакетов, подлежащих изменению порядка следования, в политике QoS с имитацией сети.

Синтаксис

```
set policy qos network-emulator <имя_политики> packet-reordering <процент>
delete policy qos network-emulator <имя_политики> packet-reordering
show policy qos network-emulator <имя_политики> packet-reordering
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      network-emulator имя_политики {
         packet-reordering процент
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики имитации сети.

процент

Процентная доля пакетов, порядок следования которых подлежит изменению случайным образом.

Значение по умолчанию

Порядок следования пакетов не изменяется (т.е. 0%).

Указания по использованию

Эта команда используется для установки процентной доли пакетов, порядок следования которых подлежит изменению, в политике QoS с имитацией сети. Изменение такого рода имитирует неисправности канала, вызывающие изменение порядка следования пакетов. Данный механизм будет работать только в случае, если в очереди имеется более одного пакета.

Форма **set** этой команды используется для указания процентной доли пакетов, порядок следования которых подлежит случайному изменению, в политике QoS с имитацией сети.

Форма **delete** этой команды используется для восстановления процентной доли по умолчанию пакетов, порядок следования которых подлежит случайному изменению, в политике QoS с имитацией сети.

Форма **show** этой команды используется для отображения настройки изменения порядка следования пакетов.

22.2.17 policy qos network-emulator <имя_политики> queue-limit <ограничение>

Установка верхней границы разрешенного числа пакетов в очереди для политики QoS с имитацией сети.

Синтаксис

```
set policy qos network-emulator <имя_политики> queue-limit <ограничение>
delete policy qos network-emulator <имя_политики> queue-limit
show policy qos network-emulator <имя_политики> queue-limit
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      network-emulator имя_политики {
         queue-limit  ограничение
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики имитации сети.

ограничение

Необязательный. Максимальный размер очереди в пакетах.

Значение по умолчанию

Длина очереди не должна превосходить 127 пакетов.

Указания по использованию

Эта команда используется для установки максимального числа пакетов, которые могут стоять в очереди, при использовании данной политики работы с очередями. Если достигнута максимальная длина очереди, система начинает отбрасывать пакеты.

Форма **set** этой команды используется для установки ограничения длины очереди.

Форма **delete** этой команды используется для восстановления длины очереди по умолчанию.

Форма **show** этой команды используется для отображения настройки ограничения длины очереди.

22.2.18 policy qos priority-queue <имя_политики>

Определение политики QoS с приоритизированной очередью.

Синтаксис

```
set policy qos priority-queue <имя_политики>
delete policy qos priority-queue <имя_политики>
show policy qos priority-queue <имя_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      priority-queue имя_политики {
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики приоритизированной очереди.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения политики QoS с приоритизированной очередью.

Политика приоритизированной очереди применима только к исходящему трафику. Имя политики должно быть уникальным и еще не использованным в других командах политик QoS. Политика приоритизированной очереди обеспечивает всем классам справедливый доступ на основе приоритизации очередей. Различие между алгоритмами управления загрузкой канала и приоритизированной очереди состоит в том, что первый ограничивает использование пропускной способности классом и затем распределяет любую оставшуюся пропускную способность. При применении политики приоритизированной очереди пакет помещается на временное хранение в очередь по заданным правилам. Как только канал связи станет доступным, маршрутизатор начнёт передачу пакетов из очереди, имеющей максимальный приоритет.

Форма **set** этой команды используется для создания политики QoS с приоритизированной очередью.

Форма **delete** этой команды используется для удаления политики QoS с приоритизированной очередью.

Форма **show** этой команды используется для отображения настройки политики QoS с приоритизированной очередью.

22.2.19 policy qos priority-queue <имя_политики> description <описание>

Указание текстового описания для политики QoS с приоритизированной очередью.

Синтаксис

```
set policy qos priority-queue <имя_политики> description <описание>
delete policy qos priority-queue <имя_политики> description
show policy qos priority-queue <имя_политики> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      priority-queue имя_политики {
         description описание
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики приоритизированной очереди.

описание

Необязательный. Описание для данной политики приоритизированной очереди.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для записи описания политики приоритизированной очереди.

Форма **set** этой команды используется для указания описания политики приоритизированной очереди.

Форма **delete** этой команды используется для удаления описания политики приоритизированной очереди.

Форма **show** этой команды используется для отображения настройки описания политики приоритизированной очереди.

22.2.20 policy qos priority-queue <имя_политики> class <класс>

Определение класса трафика для политики QoS с приоритизированной очередью.

Синтаксис

```
set policy qos priority-queue <имя_политики> class <класс>
delete policy qos priority-queue <имя_политики> class <класс>
show policy qos priority-queue <имя_политики> class <класс>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      priority-queue имя_политики {
         class класс {
         }
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики приоритизированной очереди.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 7.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения класса трафика в политике QoS с приоритизированной очередью. Такое определение позволяет группировать пакеты в разные классы трафика, обрабатываемые с разными уровнями обслуживания.

Форма **set** этой команды используется для создания класса трафика в политике QoS с приоритизированной очередью.

Форма **delete** этой команды используется для удаления класса трафика из политики QoS с приоритизированной очередью.

Форма **show** этой команды используется для отображения настройки класса трафика в политике QoS с приоритизированной очередью.

22.2.21 policy qos priority-queue <имя_политики> class <класс> description <описание>

Указание текстового описания для класса трафика.

Синтаксис

```
set policy qos priority-queue <имя_политики> class <класс> description <описание>
delete policy qos priority-queue <имя_политики> class <класс> description
show policy qos priority-queue <имя_политики> class <класс> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        priority-queue имя_политики {
            class класс {
                description описание
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики приоритизированной очереди.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 7.

описание

Необязательный. Описание для данного класса трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для записи описания класса трафика.

Форма **set** этой команды используется для указания описания.

Форма **delete** этой команды используется для удаления описания.

Форма **show** этой команды используется для отображения настройки описания.

22.2.22 policy qos priority-queue <имя_политики> class <класс> match <имя_правила>

Определение правила для проверки соответствия классов трафика.

Синтаксис

```
set policy qos priority-queue <имя_политики> class <класс> match <имя_правила>
delete policy qos priority-queue <имя_политики> class <класс> match <имя_правила>
show policy qos priority-queue <имя_политики> class <класс> match <имя_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        priority-queue имя_политики {
            class класс {
                match имя_правила {
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики приоритизированной очереди.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 7.

имя_правила

Имя правила соответствия для класса.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения правила, устанавливающего условия соответствия для членства в классе трафика.

Форма **set** этой команды используется для создания правила соответствия в классе трафика.

Форма **delete** этой команды используется для удаления узла конфигурации правила соответствия в классе трафика.

Форма **show** этой команды используется для отображения настройки правила соответствия в классе трафика.

22.2.23 policy qos priority-queue <имя_политики> class <класс> match <имя_правила> description <описание>

Указание текстового описания для правила соответствия.

Синтаксис

```
set policy qos priority-queue <имя_политики> class <класс> match <имя_правила> description <описание>
```

```
delete policy qos priority-queue <имя_политики> class <класс> match <имя_правила> description
```

```
show policy qos priority-queue <имя_политики> class <класс> match <имя_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        priority-queue имя_политики {
            class класс {
                match имя_правила {
                    description описание
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики приоритизированной очереди.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 7.

имя_правила

Необязательный. Имя правила соответствия для класса.

описание

Необязательный. Описание для данного соответствия.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для записи описания правила проверки соответствия классов трафика.

Форма **set** этой команды используется для установки описания.

Форма **delete** этой команды используется для удаления описания.

Форма **show** этой команды используется для отображения настройки описания.

22.2.24 policy qos priority-queue <имя_политики> class <класс> match <имя_правила> ether destination <mac_адрес>

Указание критерия соответствия на основе MAC-адреса получателя.

Синтаксис

```
set policy qos priority-queue <имя_политики> class <класс> match <имя_правила> ether destination <mac_адрес>
```

```
delete policy qos priority-queue <имя_политики> class <класс> match <имя_правила> ether destination
```

```
show policy qos priority-queue <имя_политики> class <класс> match <имя_правила> ether destination
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      priority-queue имя_политики {
         class класс {
            match имя_правила {
               ether {
                  destination mac_адрес
               }
            }
         }
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики приоритизированной очереди.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 7.

имя_соответствия

Имя правила соответствия для класса.

mac_адрес

MAC-адрес получателя, на соответствие которому выполняется проверка.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие MAC-адреса получателя.

Указания по использованию

Эта команда используется для определения условия соответствия по MAC-адресу получателя в классе трафика.

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для указания получателя, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления получателя в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки получателя в качестве проверяемого условия соответствия.

22.2.25 policy qos priority-queue <имя_политики> class <класс> match <имя_правила> ether protocol <тип_кадра>

Указание критерия соответствия на основе типа кадра Ethernet.

Синтаксис

```
set policy qos priority-queue <имя_политики> class <класс> match <имя_правила> ether protocol <тип_кадра>

delete policy qos priority-queue <имя_политики> class <класс> match <имя_правила> ether protocol

show policy qos priority-queue <имя_политики> class <класс> match <имя_правила> ether protocol
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        priority-queue имя_политики {
            class класс {
                match имя_правила {
                    ether {
                        protocol тип_кадра
                    }
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики приоритизированной очереди.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 7.

имя_правила

Имя правила соответствия для класса.

тип_кадра

Тип кадра Ethernet, соответствие которому проверяется, номер типа кадра должен находиться в промежутке от 0 до 65535, либо соответствовать одному из допустимых значений. Допустимые значения представлены в таблице ниже.

Таблица 184 – Допустимые типы кадров ethernet

Значение	Описание
<0-65535>	Номер типа
all	Кадр любого протокола
802.1Q	Кадр протокола 802.1Q VLAN tag
802_2	Кадр протокола 802.2
802_3	Кадр протокола 802.3

Значение	Описание
aarp	Кадр протокола Appletalk AARP
aoe	Кадр протокола ATA over Ethernet
arp	Кадр протокола Address Resolution Protocol
atalk	Кадр протокола Appletalk DDP
dec	Кадр протокола DEC
ip	Кадр протокола Internet IP (IPv4)
ipv6	Кадр протокола Internet IP (IPv6)
ipx	Кадр протокола Novell Internet Packet Exchange
lat	Кадр протокола DEC LAT
localtalk	Кадр протокола Localtalk
loop	Ethernet loopback
rarp	Кадр протокола Reverse Address Resolution Protocol
snap	Кадр протокола SNAP
x25	Кадр протокола X.25

Значение по умолчанию

Если параметр не установлен, кадры не проверяются на соответствие типа кадра Ethernet.

Указания по использованию

Это команда используется для определения условия соответствия по типу кадра Ethernet в классе трафика.

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для указания типа кадра, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления типа кадра в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки типа кадра в качестве проверяемого условия соответствия.

22.2.26 policy qos priority-queue <имя_политики> class <класс> match <имя_правила> ether source <mac_адрес>

Указание критерия соответствия на основе MAC-адреса отправителя.

Синтаксис

```
set policy qos priority-queue <имя_политики> class <класс> match <имя_правила> ether source <mac_адрес>

delete policy qos priority-queue <имя_политики> class <класс> match <имя_правила> ether source

show policy qos priority-queue <имя_политики> class <класс> match <имя_правила> ether source
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        priority-queue имя_политики {
```

```
            class класс {
               match имя_правила {
                  ether {
                     source mac_адрес
                  }
               }
            }
         }
      }
   }
```

Параметры

имя_политики

Обязательный. Имя политики приоритизированной очереди.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 7.

имя_соответствия

Имя правила соответствия для класса.

mac_адрес

MAC-адрес отправителя, на соответствие которому выполняется проверка.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие MAC-адреса отправителя.

Указания по использованию

Эта команда используется для определения условия соответствия по MAC-адресу отправителя в классе трафика.

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для указания отправителя, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления отправителя в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки отправителя в качестве проверяемого условия соответствия.

22.2.27 policy qos priority-queue <имя_политики> class <класс> match <имя_правила> interface <интерфейс>

Указание критерия соответствия на основе входного интерфейса пакетов.

Синтаксис

```
set policy qos priority-queue <имя_политики> class <класс> match
<имя_правила> interface <интерфейс>

delete policy qos priority-queue <имя_политики> class <класс> match
<имя_правила> interface

show policy qos priority-queue <имя_политики> class <класс> match
<имя_правила> interface
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        priority-queue имя_политики {
            class класс {
                match имя_правила {
                    interface интерфейс
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики приоритизированной очереди.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 7.

имя_соответствия

Имя правила соответствия для класса.

интерфейс

Имя интерфейса Ethernet, на соответствие которому выполняется проверка. С указанным значением будет сравниваться входной интерфейс пакета.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки условия соответствия по входному интерфейсу в классе трафика.

Если входящие пакеты попадают в систему через интерфейс, указанный данной командой, то трафик будет членом данного класса трафика (при условии, что другие условия соответствия удовлетворяются).

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для входного интерфейса пакетов.

Форма **delete** этой команды используется для удаления соответствия по интерфейсу.

Форма **show** этой команды используется для отображения настройки соответствия по интерфейсу.

22.2.28 policy qos priority-queue <имя_политики> class <класс> match <имя_правила> filter <имя_фильтра>

Указание критерия соответствия на основе определённого фильтра IPv4-трафика.

Синтаксис

```
set policy qos priority-queue <имя_политики> class <класс> match <имя_правила> filter <имя_фильтра>

delete policy qos priority-queue <имя_политики> class <класс> match <имя_правила> filter <имя_фильтра>

show policy qos priority-queue <имя_политики> class <класс> match <имя_правила> filter
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        priority-queue имя_политики {
            class класс {
                match имя_правила {
                    filter имя_фильтра
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики приоритизированной очереди.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 7.

имя_соответствия

Имя правила соответствия для класса.

имя_фильтра

Необязательный. Имя определённого фильтра трафика.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие сведениям о получателе.

Указания по использованию

Эта команда используется для определения условия соответствия на основе определённого фильтра IPv4-трафика в классе трафика.

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для указания фильтра трафика, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления фильтра трафика в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки фильтра трафика в качестве проверяемого условия соответствия.

22.2.29 policy qos priority-queue <имя_политики> class _<класс> match <имя_правила> filter-ipv6 <имя_фильтра>

Указание критерия соответствия на основе определённого фильтра IPv6-трафика.

Синтаксис

```
set policy qos priority-queue <имя_политики> class <класс> match <имя_правила> filter-ipv6 <имя_фильтра>

delete policy qos priority-queue <имя_политики> class <класс> match <имя_правила> filter-ipv6 <имя_фильтра>

show policy qos priority-queue <имя_политики> class <класс> match <имя_правила> filter-ipv6
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      priority-queue имя_политики {
         class класс {
            match имя_правила {
               filter-ipv6 имя_фильтра
            }
         }
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики приоритизированной очереди.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 7.

имя_соответствия

Имя правила соответствия для класса.

имя_фильтра

Необязательный. Имя определённого фильтра трафика.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие сведениям о получателе.

Указания по использованию

Эта команда используется для определения условия соответствия на основе определённого фильтра IPv6-трафика в классе трафика.

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для указания фильтра трафика, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления фильтра трафика в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки фильтра трафика в качестве проверяемого условия соответствия.

22.2.30 policy qos priority-queue <имя_политики> class <класс> match <имя_правила> vif <идентификатор_vlan>

Указание критерия соответствия на основе идентификатора VLAN.

Синтаксис

```
set policy qos priority-queue <имя_политики> class <класс> match <имя_правила> vif <идентификатор_vlan>

delete policy qos priority-queue <имя_политики> class <класс> match <имя_правила> vif

show policy qos priority-queue <имя_политики> class <класс> match <имя_правила> vif
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        priority-queue имя_политики {
            class класс {
                match имя_правила {
                    vif идентификатор_vlan
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики приоритизированной очереди.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 7.

имя_соответствия

Имя правила соответствия для класса.

идентификатор_vlan

Идентификатор VLAN, соответствие которому проверяется. Значение должно находиться в диапазоне от 1 до 4094.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие идентификатору VLAN.

Указания по использованию

Это команда используется для определения условия соответствия по идентификатору VLAN в классе трафика.

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для указания идентификатора VLAN, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления идентификатора VLAN в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки идентификатора VLAN в качестве проверяемого условия соответствия.

22.2.31 policy qos priority-queue <имя_политики> class <класс> queue-limit <ограничение>

Указание максимального размера очереди для класса трафика.

Синтаксис

```
set policy qos priority-queue <имя_политики> class <класс> queue-limit <ограничение>

delete policy qos priority-queue <имя_политики> class <класс> queue-limit

show policy qos priority-queue <имя_политики> class <класс> queue-limit
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        priority-queue имя_политики {
            class класс {
                queue-limit ограничение
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики приоритизированной очереди.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 7.

ограничение

Максимальный размер очереди в пакетах.

Значение по умолчанию

Значение ограничения по умолчанию равно 127.

Указания по использованию

Эта команда используется для установки максимального размера очереди (в пакетах) в классе трафика.

Форма **set** этой команды используется для указания ограничения длины очереди.

Форма **delete** этой команды используется для удаления ограничения длины очереди.

Форма **show** этой команды используется для отображения настройки ограничения длины очереди.

22.2.32 policy qos priority-queue <имя_политики> class <класс> queue-ref <имя_политики>

Указание дочерней политики QoS для данного класса трафика.

Синтаксис

```
set policy qos priority-queue <имя_политики> class <класс> queue-ref <имя_политики>
delete policy qos priority-queue <имя_политики> class <класс> queue-ref <имя_политики>
show policy qos priority-queue <имя_политики> class <класс> queue-ref
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        priority-queue имя_политики {
            class класс {
                queue-ref имя_политики
            }
        }
    }
}
```

Параметры

priority-queue *имя_политики*

Обязательный. Имя политики приоритизированной очереди.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 7.

queue-ref *имя_политики*

Необязательный. Имя дочерней политики QoS.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки дочерней политики QoS. Данная дочерняя политика будет применяться к трафику, попавшему в указанный класс.

Форма **set** этой команды используется для указания дочерней политики QoS.

Форма **delete** этой команды используется для удаления дочерней политики QoS.

Форма **show** этой команды используется для отображения настройки использования дочерней политики QoS.

22.2.33 policy qos priority-queue <имя_политики> class <класс> queue-type <тип>

Указание типа работы с очередью, используемого для класса трафика.

Синтаксис

```
set policy qos priority-queue <имя_политики> class <класс> queue-type <тип>
delete policy qos priority-queue <имя_политики> class <класс> queue-type
show policy qos priority-queue <имя_политики> class <класс> queue-type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      priority-queue имя_политики {
         class класс {
            queue-type тип
         }
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики приоритизированной очереди.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 7.

имя_соответствия

Имя правила соответствия для класса.

тип

Используемый метод работы с очередями. Допустимые значения представлены в таблице ниже.

Таблица 185 – Допустимые типы очередей

Значение	Описание
fair-queue	Используется очередь SFQ.
drop-tail	Используется очередь FIFO.
priority	Приоритет в очереди устанавливается по значениям поля DSCP в байте ToS заголовка IP.
random-detect	Используется очередь RED.

Значение по умолчанию

По умолчанию используется тип fair-queue.

Указания по использованию

Эта команда используется для установки типа механизма работы с очередями, используемого в классе трафика.

Форма **set** этой команды используется для указания типа очереди.

Форма **delete** этой команды используется для восстановления типа очереди по умолчанию.

Форма **show** этой команды используется для отображения настройки типа очереди.

22.2.34 policy qos priority-queue <имя_политики> default

Определение политики QoS по умолчанию с приоритизированной очередью.

Синтаксис

```
set policy qos priority-queue <имя_политики> default
delete policy qos priority-queue <имя_политики> default
show policy qos priority-queue <имя_политики> default
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      priority-queue <имя_политики> {
         default {
         }
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики приоритизированной очереди.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения политики приоритизированной очереди по умолчанию. Эта политика будет применена ко всему трафику, не соответствующему никакому другому определенному классу.

Форма **set** этой команды используется для создания узла конфигурации класса по умолчанию.

Форма **delete** этой команды используется для удаления узла конфигурации класса по умолчанию.

Форма **show** этой команды используется для отображения узла конфигурации класса по умолчанию.

22.2.35 policy qos priority-queue <имя_политики> default queue-limit <ограничение>

Указание максимального размера очереди для класса трафика по умолчанию.

Синтаксис

```
set policy qos priority-queue <имя_политики> default queue-limit <ограничение>
delete policy qos priority-queue <имя_политики> default queue-limit
show policy qos priority-queue <имя_политики> default queue-limit
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      priority-queue имя_политики {
```

```
            default {
                queue-limit ограничение
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики приоритизированной очереди.

ограничение

Максимальный размер очереди в пакетах.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки максимального размера (в пакетах) очереди класса по умолчанию.

Форма **set** этой команды используется для указания ограничения длины очереди.

Форма **delete** этой команды используется для удаления ограничения длины очереди.

Форма **show** этой команды используется для отображения настройки ограничения длины очереди.

22.2.36 policy qos priority-queue <имя_политики> default queue-ref <имя_политики>

Указание дочерней политики QoS по умолчанию.

Синтаксис

```
set policy qos priority-queue <имя_политики> default queue-ref <имя_политики>
delete policy qos priority-queue <имя_политики> default queue-ref
show policy qos priority-queue <имя_политики> default queue-ref
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        priority-queue имя_политики {
            default {
                queue-ref имя_политики
            }
        }
    }
}
```

Параметры

priority-queue *имя_политики*

Обязательный. Имя политики приоритизированной очереди.

queue-ref *имя_политики*

Необязательный. Имя дочерней политики QoS.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки дочерней политики QoS по умолчанию. Данная дочерняя политика будет применяться ко всему трафику, не соответствующему никакому другому определённому классу в рамках указанной политики.

Форма **set** этой команды используется для указания дочерней политики QoS.

Форма **delete** этой команды используется для удаления дочерней политики QoS.

Форма **show** этой команды используется для отображения настройки использования дочерней политики QoS.

22.2.37 policy qos priority-queue <имя_политики> default queue-type <тип>

Указание типа работы с очередью, используемого для класса трафика по умолчанию.

Синтаксис

```
set policy qos priority-queue <имя_политики> default queue-type <тип>
delete policy qos priority-queue <имя_политики> default queue-type
show policy qos priority-queue <имя_политики> default queue-type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      priority-queue имя_политики {
         default {
            queue-type тип
         }
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики приоритизированной очереди.

тип

Используемый метод работы с очередями. Допустимые значения представлены в таблице ниже.

Таблица 186 – Допустимые типы очередей

Значение	Описание
fair-queue	Используется очередь SFQ.
drop-tail	Используется очередь FIFO.
priority	Приоритет в очереди устанавливается по значениям поля DSCP в байте ToS заголовка IP.
random-detect	Используется очередь RED.

Значение по умолчанию

По умолчанию используется тип fair-queue.

Указания по использованию

Эта команда используется для установки типа механизма работы с очередями, используемого в классе трафика по умолчанию.

Форма **set** этой команды используется для указания типа очереди.

Форма **delete** этой команды используется для восстановления типа очереди по умолчанию.

Форма **show** этой команды используется для отображения настройки типа очереди.

22.2.38 policy qos random-detect <имя_политики>

Определение политики QoS со взвешенным случайным ранним определением (WRED).

Синтаксис

```
set policy qos random-detect <имя_политики>
delete policy qos random-detect <имя_политики>
show policy qos random-detect <имя_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      random-detect имя_политики {
      }
   }
}
```

Параметры

имя_политики

Формат – текст. Обязательный. Имя политики случайного определения.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения политики QoS со случайным определением, основанной на механизме WRED предотвращения перегрузки. Политика случайного определения очереди применима только к исходящему трафику. Имя политики должно быть уникальным и еще не использованным в других командах политик QoS.

Механизм RED (Random Early Detection, случайное раннее определение) случайным образом отбрасывает пакеты перед периодами высокой загрузки, чтобы подать отправителю пакетов сигнал о необходимости снизить скорость передачи. Такие действия помогают предотвратить условия, при которых выходные буферы заполняются и пакеты в конце буфера (как и пакеты, вновь прибывающие в буфер) отбрасываются. Отбрасывание может вызвать глобальную пересинхронизацию узлов TCP, так как несколько узлов снижают скорость передачи. После ликвидации перегрузки скорости передачи снова увеличивается до тех пор, пока перегрузка не наступит снова. Такой цикл из перегрузки и ее ликвидации не способствует наилучшему использованию доступной пропускной способности сети. Механизм RED уменьшает вероятность наступления перегрузки путем избирательного отбрасывания пакетов при условии, что на выходном интерфейсе появляются признаки перегрузки. Оно в свою очередь уменьшает вероятность глобальной синхронизации и позволяет лучше использовать доступную пропускную способность.

WRED - это расширение RED, позволяющее добавить предпочтительность к различным потокам трафика и тем самым обеспечить различное качество обслуживания различным потокам трафика путем отбрасывания из одних потоков большего числа пакетов, чем из других.

Форма **set** этой команды используется для создания политики QoS со случайным определением.

Форма **delete** этой команды используется для удаления политики QoS со случайным определением.

Форма **show** этой команды используется для отображения настройки политики QoS со случайным определением.

22.2.39 policy qos random-detect <имя_политики> bandwidth <скорость>

Указание ограничения пропускной способности для всего суммарного трафика, ограничиваемого данной политикой.

Синтаксис

```
set policy qos random-detect <имя_политики> bandwidth <скорость>
delete policy qos random-detect <имя_политики> bandwidth
show policy qos random-detect <имя_политики> bandwidth
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      random-detect имя_политики {
         bandwidth скорость
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики случайного определения.

скорость

Пропускная способность. Допустимые форматы представлены в таблице ниже.

Таблица 187 – Формат указания пропускной способности

Значение	Описание
auto	Пропускная способность основана на скорости интерфейса
<число>	Пропускная способность указанная в килобайтах в секунду.
<число><приставка>	Пропускная способность в указанных единицах измерения. Поддерживаются следующие единицы измерения: **kbit:** килобит в секунду. **mbit:** мегабит в секунду. **gbit:** гигабит в секунду. **kbps:** килобайт в секунду. **mbps:** мегабайт в секунду. **gbps:** гигабайт в секунду.

Значение по умолчанию

Пропускная способность основана на интерфейсе, к которому применяется политика.

Указания по использованию

Эта команда используется для установки ограничений на пропускную способность в политике QoS со случайным определением. Данный параметр описывает максимальную пропускную способность, доступную всем классам.

ПРИМЕЧАНИЕ Автоматическое определение скорости интерфейса доступно лишь для интерфейсов типа Ethernet. При отсутствии автоматического определения (например, не подключен кабель) будет использовано значение по умолчанию. В случае невозможности автоматического определения скорости выводится предупреждение об использовании соответствующего значения по умолчанию, однако, на некоторых аппаратных платформах его может не быть. В связи с этим автоматическое определение не является рекомендуемым значением.

Форма **set** этой команды используется для указания ограничений пропускной способности для политики.

Форма **delete** этой команды используется для восстановления ограничений пропускной способности по умолчанию.

Форма **show** этой команды используется для отображения настройки пропускной способности, выделенной политике.

22.2.40 policy qos random-detect <имя_политики> description <описание>

Указание текстового описания для политики случайного определения.

Синтаксис

```
set policy qos random-detect <имя_политики> description <описание>
delete policy qos random-detect и<имя_политики> description
show policy qos random-detect <имя_политики> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      random-detect имя_политики {
         description описание
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики случайного определения.

описание

Необязательный. Описание для данной политики случайного определения.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для записи описания политики случайного определения.

Форма **set** этой команды используется для указания описания.

Форма **delete** этой команды используется для удаления описания.

Форма **show** этой команды используется для отображения настройки описания.

22.2.41 policy qos random-detect <имя_политики> precedence <предпочтительность>

Установка параметров отбрасывания пакетов на основе предпочтительности для политики случайного определения.

Синтаксис

```
set policy qos random-detect <имя_политики> precedence <предпочтительность> [average-packet <байты> | mark-probability <вероятность> | maximum-threshold <максимум> | minimum-threshold <минимум> | queue-limit <число_пакетов>]

delete policy qos random-detect <имя_политики> precedence <предпочтительность> [average-packet | mark-probability | maximum-threshold | minimum-threshold | queue-limit]

show policy qos random-detect <имя_политики> precedence <предпочтительность> [average-packet | mark-probability | maximum-threshold | minimum-threshold | queue-limit]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        random-detect имя_политики {
            precedence предпочтительность {
                average-packet байты
                mark-probability вероятность
                maximum-threshold максимум
                minimum-threshold минимум
                queue-limit число_пакетов
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики случайного определения.

предпочтительность

Предпочтительность IP (первые три бита поля TOS) пакета. Значение должно находиться в диапазоне от 0 до 7.

байты

Средний размер пакета в байтах. Значение должно находиться в диапазоне от 16 до 10240 пакетов. Значение по умолчанию равно 1024.

вероятность

Доля пакетов (т.е. 1/вероятность), отбрасываемая, когда средняя глубина очереди достигает максимального порога. Значение по умолчанию равно 10.

максимум

Когда средняя глубина очереди превосходит указанное значение, отбрасываются все пакеты. Значение должно находиться в диапазоне от 0 до 4096 пакетов. Значение по умолчанию равно 18.

минимум

Когда средняя глубина очереди достигает указанного значения, пакеты начинают отбрасываться. Значение должно находиться в диапазоне от 0 до 4096 пакетов. Значение по умолчанию зависит от предпочтительности:

- Предпочтительность 0 -> min-threshold = 9
- Предпочтительность 1-> min-threshold = 10
- Предпочтительность 2 -> min-threshold = 11
- Предпочтительность 3 -> min-threshold = 12
- Предпочтительность 4 -> min-threshold = 13
- Предпочтительность 5 -> min-threshold = 14
- Предпочтительность 6 -> min-threshold = 15
- Предпочтительность 7 -> min-threshold = 16

число_пакетов

Когда мгновенная глубина очереди достигает указанного значения, отбрасываются все пакеты. Значение по умолчанию равно 4 * max-threshold.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания параметров отбрасывания пакетов в политике случайного определения.

Для классификации потоков данных в указанной функции используются первые три бита поля TOS (тип обслуживания). Внутри каждого из потоков можно установить параметры для настройки скорости, при которой начинается отбрасывание пакетов в случае перегрузки. Каждый раз, когда приходит пакет для отправки вовне через интерфейс, принимается решение на основе предпочтительности пакета и параметров, установленных для указанной предпочтительности. Если средняя длина выходной очереди меньше, чем min-threshold, пакет помещается в выходную очередь. Если средняя длина выходной очереди находится между min-threshold и max-threshold, пакет может быть поставлен в очередь или отброшен в зависимости от значения параметра вероятность. Если средняя длина выходной очереди больше параметра max-threshold, все пакеты отбрасываются. Если мгновенная длина очереди превосходит значение параметра queue-limit, все пакеты отбрасываются.

Если параметр max-threshold установлен, а параметр min-threshold нет, то min-threshold автоматически устанавливается на 1/2 max-threshold. Кроме того, система автоматически выполняет следующее ограничение:

min-threshold < max-threshold > queue-limit.

ПРИМЕЧАНИЕ Пакеты протоколов, отличных от IP, воспринимаются как имеющие предпочтительность 0.

Форма **set** этой команды используется для указания параметров отбрасывания пакетов в политике случайного определения.

Форма **delete** этой команды используется для удаления параметров отбрасывания пакетов в политике случайного определения.

Форма **show** этой команды используется для отображения параметров отбрасывания пакетов в политике случайного определения.

22.2.42 policy qos rate-control <имя_политики>

Определение политики QoS с ограничением скорости.

Синтаксис

```
set policy qos rate-control <имя_политики>
delete policy qos rate-control <имя_политики>
show policy qos rate-control <имя_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
```

```
    qos {
        rate-control имя_политики {
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения скорости.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения политики QoS с ограничением скорости. Политика ограничения скорости применима только к исходящему трафику. Имя политики должно быть уникальным и еще не использованным в других командах политик QoS.

В Numa Edge используется вариант алгоритма "маркерного ведра" (Token Bucket Filter, TBF). TBF - это бесклассовая дисциплина работы с очередями, пропускающая только пакеты, приходящие со скоростью, не превосходящей административно установленной скорости, но с возможностью коротких серий, превосходящих эту скорость ("всплесков").

Форма **set** этой команды используется для создания политики QoS с ограничением скорости. До фиксации настройки для данной политики обязательно должен быть определен параметр bandwidth, в противном случае фиксация завершится сбоем.

Форма **delete** этой команды используется для удаления политики QoS с ограничением скорости.

Форма **show** этой команды используется для отображения настройки политики QoS с ограничением скорости.

22.2.43 policy qos rate-control <имя_политики> bandwidth <скорость>

Указание ограничения пропускной способности для всего суммарного трафика, ограничиваемого данной политикой.

Синтаксис

```
set policy qos rate-control <имя_политики> bandwidth <скорость>
delete policy qos rate-control <имя_политики> bandwidth
show policy qos rate-control <имя_политики> bandwidth
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        rate-control имя_политики {
            bandwidth скорость
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения скорости.

скорость

Пропускная способность. Допустимые форматы представлены в таблице ниже.

Таблица 188 – Формат указания пропускной способности

Значение	Описание
auto	Пропускная способность основана на скорости интерфейса
<число>	Пропускная способность указанная в килобайтах в секунду.
<число><приставка>	Пропускная способность в указанных единицах измерения. Поддерживаются следующие единицы измерения: **kbit:** килобит в секунду. **mbit:** мегабит в секунду. **gbit:** гигабит в секунду. **kbps:** килобайт в секунду. **mbps:** мегабайт в секунду. **gbps:** гигабайт в секунду.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки ограничений пропускной способности в политике QoS с ограничением скорости. Данный параметр описывает максимальную пропускную способность, доступную всем классам; он обязательно должен быть установлен.

Форма **set** этой команды используется для указания ограничений пропускной способности для политики.

Форма **delete** этой команды используется для восстановления ограничений пропускной способности по умолчанию.

Форма **show** этой команды используется для отображения настройки пропускной способности, выделенной политике.

22.2.44 policy qos rate-control <имя_политики> burst <размер>

Установка размера непрерывной серии пакетов для политики QoS с ограничением скорости.

Синтаксис

```
set policy qos rate-control <имя_политики> burst <размер>
delete policy qos rate-control <имя_политики> burst
show policy qos rate-control <имя_политики> burst
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      rate-control имя_политики {
         burst размер
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения скорости.

размер

Необязательный. Размер непрерывной серии. Размер непрерывной серии должен находиться в промежутке между 15 КБ и 32 МБ. Допустимые форматы представлены в таблице ниже.

Таблица 189 – Формат указания размера непрерывной серии.

Значение	Описание
<число>	Размер непрерывной серии указанный в байтах.
<число><приставка>	Размер непрерывной серии в указанных единицах измерения. Поддерживаются следующие единицы измерения: **kb:** килобайты. **mb:** мегабайты.

Значение по умолчанию

Длина непрерывной серии по умолчанию 15 килобайт.

Указания по использованию

Эта команда используется для установки размера непрерывной серии пакетов в политике QoS с ограничением скорости. Устанавливается максимальный объем трафика, который может быть передан за один раз.

Форма **set** этой команды используется для указания размера непрерывной серии пакетов в политике QoS с ограничением скорости.

Форма **delete** этой команды используется для восстановления размера непрерывной серии по умолчанию в политике QoS с ограничением скорости.

Форма **show** этой команды используется для отображения настройки размера непрерывной серии в политике ограничения скорости.

22.2.45 policy qos rate-control <имя_политики> description <описание>

Указание текстового описания для политики ограничения скорости.

Синтаксис

```
set policy qos rate-control <имя_политики> description <описание>
delete policy qos rate-control <имя_политики> description
show policy qos rate-control <имя_политики> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      rate-control имя_политики {
         description описание
      }
   }
}
```

Параметры

имя_политики

Имя политики ограничения скорости.

описание

Описание для данной политики ограничения скорости.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для записи описания политики ограничения скорости.

Форма **set** этой команды используется для указания описания.

Форма **delete** этой команды используется для удаления описания.

Форма **show** этой команды используется для отображения настройки описания.

22.2.46 policy qos rate-control <имя_политики> latency <задержка>

Установка ограничения на размер очереди на основе задержки для политики QoS с ограничением скорости.

Синтаксис

```
set policy qos rate-control <имя_политики> latency <задержка>
delete policy qos rate-control <имя_политики> latency
show policy qos rate-control <имя_политики> latency
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      rate-control имя_политики {
         latency задержка
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения скорости.

задержка

Задержка между пакетами. Допустимые форматы:

Таблица 190 – Формат указания задержки между пакетами.

Значение	Описание
<число>	Задержка между пакетами в секундах.
<число><приставка>	Задержка между пакетами в указанных единицах измерения. Поддерживаются следующие единицы измерения: **secs:** секунды. **ms:** миллисекунды. **us:** микросекунды.

Значение по умолчанию

По умолчанию задержка составляет 50 миллисекунд.

Указания по использованию

Эта команда используется для установки задержки в политике QoS с ограничением скорости. Указывается максимальное время, которое пакет может находиться в "маркерном ведре".

Форма **set** этой команды используется для указания задержки в политике QoS с ограничением скорости.

Форма **delete** этой команды используется для восстановления задержки по умолчанию в политике QoS с ограничением скорости.

Форма **show** этой команды используется для отображения настройки задержки в политике QoS с ограничением скорости.

22.2.47 policy qos round-robin <имя_политики>

Определение политики QoS с циклическим перебором.

Синтаксис

```
set policy qos round-robin <имя_политики>
delete policy qos round-robin <имя_политики>
show policy qos round-robin <имя_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      round-robin имя_политики {
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики циклического перебора.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения политики QoS с циклическим перебором. Политика циклического перебора применима только к исходящему трафику. Имя политики должно быть уникальным и еще не использованным в других командах политик QoS.

Политика циклического перебора обеспечивает всем классам справедливый доступ на основе циклического перебора. Различие между алгоритмами управления загрузкой канала и циклического перебора состоит в том, что первый ограничивает использование пропускной способности классом и затем распределяет любую оставшуюся пропускную способность. Напротив, при циклическом переборе делается попытка разделить пропускную способность между определенными классами.

Форма **set** этой команды используется для создания политики QoS с циклическим перебором.

Форма **delete** этой команды используется для удаления политики QoS с циклическим перебором.

Форма **show** этой команды используется для отображения настройки политики QoS с циклическим перебором.

22.2.48 policy qos round-robin <имя_политики> description <описание>

Указание текстового описания для политики QoS с циклическим перебором.

Синтаксис

set policy qos round-robin <имя_политики> description <описание>

delete policy qos round-robin <имя_политики> description

show policy qos round-robin <имя_политики> description

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      round-robin имя_политики {
         description описание
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики циклического перебора.

описание

Необязательный. Описание для данной политики циклического перебора.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для записи описания политики циклического перебора.

Форма **set** этой команды используется для указания описания политики циклического перебора.

Форма **delete** этой команды используется для удаления описания политики циклического перебора.

Форма **show** этой команды используется для отображения настройки описания политики циклического перебора.

22.2.49 policy qos round-robin <имя_политики> class <класс>

Определение класса трафика для политики QoS с циклическим перебором.

Синтаксис

```
set policy qos round-robin <имя_политики> class <класс>
delete policy qos round-robin <имя_политики> class <класс>
show policy qos round-robin <имя_политики> class <класс>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      round-robin имя_политики {
         class класс {
         }
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики циклического перебора.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4095

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения класса трафика в политике QoS с циклическим перебором. Такое определение позволяет группировать пакеты в разные классы трафика, обрабатываемые с разными уровнями обслуживания.

Форма **set** этой команды используется для создания класса трафика в политике QoS с циклическим перебором.

Форма **delete** этой команды используется для удаления класса трафика из политики QoS с циклическим перебором.

Форма **show** этой команды используется для отображения настройки класса трафика в политике QoS с циклическим перебором.

22.2.50 policy qos round-robin <имя_политики> class <класс> description <описание>

Указание текстового описания для класса трафика.

Синтаксис

```
set policy qos round-robin <имя_политики> class <класс> description <описание>
delete policy qos round-robin <имя_политики> class <класс> description
show policy qos round-robin <имя_политики> class <класс> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        round-robin имя_политики {
            class класс {
                description описание
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики циклического перебора.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4095

описание

Необязательный. Описание для данного класса трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для записи описания класса трафика.

Форма **set** этой команды используется для указания описания.

Форма **delete** этой команды используется для удаления описания.

Форма **show** этой команды используется для отображения настройки описания.

22.2.51 policy qos round-robin <имя_политики> class <класс> match <имя_правила>

Определение правила для проверки соответствия классов трафика.

Синтаксис

```
set policy qos round-robin <имя_политики> class <класс> match <имя_правила>

delete policy qos round-robin <имя_политики> class <класс> match <имя_правила>

show policy qos round-robin <имя_политики> class <класс> match <имя_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      round-robin имя_политики {
         class класс {
            match имя_правила {
            }
         }
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики циклического перебора.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4095.

имя_правила

Имя правила соответствия для класса.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения правила, устанавливающего условия соответствия для членства в классе трафика.

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для создания правила соответствия в классе трафика.

Форма **delete** этой команды используется для удаления узла конфигурации правила соответствия в классе трафика.

Форма **show** этой команды используется для отображения настройки правила соответствия в классе трафика.

22.2.52 policy qos round-robin <имя_политики> class <класс> match <имя_правила> description <описание>

Указание текстового описания для правила соответствия.

Синтаксис

```
set policy qos round-robin <имя_политики> class <класс> match <имя_правила> description <описание>

delete policy qos round-robin <имя_политики> class <класс> match <имя_правила> description

show policy qos round-robin <имя_политики> class <класс> match <имя_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        round-robin имя_политики {
            class класс {
                match имя_правила {
                    description описание
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики циклического перебора.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4095.

имя_правила

Имя правила соответствия для класса.

описание

Описание для данного соответствия.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для записи описания правила проверки соответствия классов трафика.

Форма **set** этой команды используется для установки описания.

Форма **delete** этой команды используется для удаления описания.

Форма **show** этой команды используется для отображения настройки описания.

22.2.53 policy qos round-robin <имя_политики> class <класс> match <имя_правила> ether destination <mac_адрес>

Указание критерия соответствия на основе MAC-адреса получателя.

Синтаксис

```
set policy qos round-robin <имя_политики> class <класс> match <имя_правила> ether destination <mac_адрес>

delete policy qos round-robin <имя_политики> class <класс> match <имя_правила> ether destination

show policy qos round-robin <имя_политики> class <класс> match <имя_правила> ether destination
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        round-robin имя_политики {
            class класс {
                match имя_правила {
                    ether {
                        destination mac_адрес
                    }
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики циклического перебора.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4095.

имя_соответствия

Необязательный. Имя правила соответствия для класса.

mac_адрес

Необязательный. MAC-адрес получателя, на соответствие которому выполняется проверка.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие MAC-адреса получателя.

Указания по использованию

Эта команда используется для определения условия соответствия по MAC-адресу получателя в классе трафика.

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для указания получателя, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления получателя в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки получателя в качестве проверяемого условия соответствия.

22.2.54 policy qos round-robin <имя_политики> class <класс> match <имя_правила> ether protocol <тип_кадра>

Указание критерия соответствия на основе типа кадра Ethernet.

Синтаксис

```
set policy qos round-robin <имя_политики> class <класс> match <имя_правила> ether protocol <тип_кадра>

delete policy qos round-robin <имя_политики> class <класс> match <имя_правила> ether protocol

show policy qos round-robin <имя_политики> class <класс> match <имя_правила> ether protocol
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        round-robin имя_политики {
            class класс {
                match имя_правила {
                    ether {
                        protocol тип_кадра
                    }
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики циклического перебора.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4095.

имя_правила

Имя правила соответствия для класса.

тип_кадра

Тип кадра Ethernet, соответствие которому проверяется, номер типа кадра должен находиться в промежутке от 0 до 65535, либо соответствовать одному из допустимых значений. Допустимые значения представлены в таблице ниже.

Таблица 191 – Допустимые типы кадров ethernet

Значение	**Описание**
<0-65535>	Номер типа
all	Кадр любого протокола
802.1Q	Кадр протокола 802.1Q VLAN tag
802_2	Кадр протокола 802.2
802_3	Кадр протокола 802.3
aarp	Кадр протокола Appletalk AARP
aoe	Кадр протокола ATA over Ethernet
arp	Кадр протокола Address Resolution Protocol
atalk	Кадр протокола Appletalk DDP
dec	Кадр протокола DEC
ip	Кадр протокола Internet IP (IPv4)
ipv6	Кадр протокола Internet IP (IPv6)
ipx	Кадр протокола Novell Internet Packet Exchange
lat	Кадр протокола DEC LAT
localtalk	Кадр протокола Localtalk
loop	Ethernet loopback
rarp	Кадр протокола Reverse Address Resolution Protocol
snap	Кадр протокола SNAP
x25	Кадр протокола X.25

Значение по умолчанию

Если параметр не установлен, кадры не проверяются на соответствие типа кадра Ethernet.

Указания по использованию

Эта команда используется для определения условия соответствия по типу кадра Ethernet в классе трафика.

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для указания типа кадра, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления типа кадра в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки типа кадра в качестве проверяемого условия соответствия.

22.2.55 policy qos round-robin <имя_политики> class <класс> match <имя_правила> ether source <mac_адрес>

Указание критерия соответствия на основе MAC-адреса отправителя.

Синтаксис

```
set policy qos round-robin <имя_политики> class <класс> match <имя_правила>
ether source <mac_адрес>
```

```
delete policy qos round-robin <имя_политики> class <класс> match <имя_правила> ether source
```

```
show policy qos round-robin <имя_политики> class <класс> match <имя_правила> ether source
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        round-robin имя_политики {
            class класс {
                match имя_соответствия {
                    ether {
                        source mac_адрес
                    }
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики циклического перебора.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4095.

имя_соответствия

Имя правила соответствия для класса.

mac_адрес

MAC-адрес отправителя, на соответствие которому выполняется проверка.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие MAC-адреса отправителя.

Указания по использованию

Эта команда используется для определения условия соответствия по MAC-адресу отправителя в классе трафика.

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для указания отправителя, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления отправителя в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки отправителя в качестве проверяемого условия соответствия.

22.2.56 policy qos round-robin <имя_политики> class <класс> match <имя_правила> interface <интерфейс>

Указание критерия соответствия на основе входного интерфейса пакетов.

Синтаксис

```
set policy qos round-robin <имя_политики> class <класс> match <имя_правила> interface <интерфейс>

delete policy qos round-robin <имя_политики> class <класс> match <имя_правила> interface

show policy qos round-robin <имя_политики> class <класс> match <имя_правила> interface
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        round-robin имя_политики {
            class класс {
                match имя_правила {
                    interface интерфейс
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики циклического перебора.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4095.

имя_соответствия

Имя правила соответствия для класса.

интерфейс

Имя интерфейса Ethernet, на соответствие которому выполняется проверка. С указанным значением будет сравниваться входной интерфейс пакета.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки условия соответствия по входному интерфейсу в классе трафика. Если входящие пакеты попадают в систему через интерфейс, указанный данной командой, то трафик будет членом данного класса трафика (при условии, что другие условия соответствия удовлетворяются).

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для указания входного интерфейса пакетов.

Форма **delete** этой команды используется для удаления соответствия по интерфейсу.

Форма **show** этой команды используется для отображения настройки соответствия по интерфейсу.

22.2.57 policy qos round-robin <имя_политики> class <класс> match <имя_правила> filter <имя_фильтра>

Указание критерия соответствия на основе определённого фильтра IPv4-трафика.

Синтаксис

```
set policy qos round-robin <имя_политики> class <класс> match <имя_правила> filter <имя_фильтра>

delete policy qos round-robin <имя_политики> class <класс> match <имя_правила> filter <имя_фильтра>

show policy qos round-robin <имя_политики> class <класс> match <имя_правила> filter
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        round-robin имя_политики {
            class класс {
                match имя_правила {
                    filter имя_фильтра
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики циклического перебора.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4095.

имя_соответствия

Имя правила соответствия для класса.

имя_фильтра

Необязательный. Имя определённого фильтра трафика.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие сведениям о получателе.

Указания по использованию

Эта команда используется для определения условия соответствия на основе определённого фильтра IPv4-трафика в классе трафика.

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для указания фильтра трафика, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления фильтра трафика в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки фильтра трафика в качестве проверяемого условия соответствия.

22.2.58 policy qos round-robin <имя_политики> class <класс> match <имя_правила> filter-ipv6 <имя_фильтра>

Указание критерия соответствия на основе определённого фильтра IPv6-трафика.

Синтаксис

```
set policy qos round-robin <имя_политики> class <класс> match <имя_правила> filter-ipv6 <имя_фильтра>

delete policy qos round-robin <имя_политики> class <класс> match <имя_правила> filter-ipv6 <имя_фильтра>

show policy qos round-robin <имя_политики> class <класс> match <имя_правила> filter-ipv6
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        round-robin имя_политики {
            class класс {
                match имя_правила {
                    filter-ipv6 имя_фильтра
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики циклического перебора.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4095.

имя_соответствия

Имя правила соответствия для класса.

имя_фильтра

Необязательный. Имя определённого фильтра трафика.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие сведениям о получателе.

Указания по использованию

Эта команда используется для определения условия соответствия на основе определённого фильтра IPv6-трафика в классе трафика.

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для указания фильтра трафика, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления фильтра трафика в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки фильтра трафика в качестве проверяемого условия соответствия.

22.2.59 policy qos round-robin <имя_политики> class <класс> match <имя_правила> vif <идентификатор_vlan>

Указание критерия соответствия на основе идентификатора VLAN.

Синтаксис

```
set policy qos round-robin <имя_политики> class <класс> match <имя_правила> vif <идентификатор_vlan>

delete policy qos round-robin <имя_политики> class <класс> match <имя_правила> vif

show policy qos round-robin <имя_политики> class <класс> match <имя_правила> vif
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        round-robin имя_политики {
            class класс {
                match имя_правила {
                    vif идентификатор_vlan
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики циклического перебора.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4095.

имя_соответствия

Имя правила соответствия для класса.

идентификатор_vlan

Идентификатор VLAN, соответствие которому проверяется. Значение должно находиться в диапазоне от 1 до 4094.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие идентификатору VLAN.

Указания по использованию

Это команда используется для определения условия соответствия по идентификатору VLAN в классе трафика.

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для указания идентификатора VLAN, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления идентификатора VLAN в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки идентификатора VLAN в качестве проверяемого условия соответствия.

22.2.60 policy qos round-robin <имя_политики> class <класс> quantum <число_пакетов>

Указание числа пакетов, которые могут быть отправлены за квант планирования.

Синтаксис

```
set policy qos round-robin <имя_политики> class <класс> quantum <число_пакетов>

delete policy qos round-robin <имя_политики> class <класс> quantum

show policy qos round-robin <имя_политики> class <класс> quantum
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        round-robin имя_политики {
            class класс
                quantum число_пакетов
            }
        }
```

```
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики циклического перебора.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4095.

число_пакетов

Необязательный. Число пакетов, которые могут быть отправлены за квант планирования. Значение должно лежать в диапазоне 1-4294967295.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки числа пакетов, которые могут быть отправлены за квант планирования в политике QoS с циклическим перебором.

Форма **set** этой команды используется для указания числа пакетов, которые могут быть отправлены за квант планирования.

Форма **delete** этой команды используется для удаления настройки кванта.

Форма **show** этой команды используется для отображения настройки кванта.

22.2.61 policy qos round-robin <имя_политики> class <класс> queue-limit <ограничение>

Указание максимального размера очереди для класса трафика.

Синтаксис

```
set policy qos round-robin <имя_политики> class <класс> queue-limit <ограничение>
delete policy qos round-robin <имя_политики> class <класс> queue-limit
show policy qos round-robin <имя_политики> class <класс> queue-limit
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        round-robin имя_политики {
            class класс {
                queue-limit ограничение
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики циклического перебора.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4095.

ограничение

Максимальный размер очереди в пакетах. Значение должно лежать в диапазоне 2-4294967295.

Значение по умолчанию

Значение ограничения по умолчанию равно 127.

Указания по использованию

Эта команда используется для установки максимального размера очереди (в пакетах) в классе трафика.

Форма **set** этой команды используется для указания ограничения длины очереди.

Форма **delete** этой команды используется для удаления ограничения длины очереди.

Форма **show** этой команды используется для отображения настройки ограничения длины очереди.

22.2.62 policy qos round-robin <имя_политики> class <класс> queue-ref <имя_политики>

Указание дочерней политики QoS для данного класса трафика.

Синтаксис

```
set policy qos round-robin <имя_политики> class <класс> queue-ref <имя_дочерней_политики>

delete policy qos round-robin <имя_политики> class <класс> queue-ref <имя_дочерней_политики>

show policy qos round-robin <имя_политики> class <класс> queue-ref
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      round-robin имя_политики {
         class класс {
            queue-ref имя_дочерней_политики
         }
      }
   }
}
```

Параметры

round-robin *имя_политики*

Обязательный. Имя политики циклического перебора.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4095.

queue-ref *имя_политики*

Необязательный. Имя дочерней политики QoS.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки дочерней политики QoS. Данная дочерняя политика будет применяться к трафику, попавшему в указанный класс.

Форма **set** этой команды используется для указания дочерней политики QoS.

Форма **delete** этой команды используется для удаления дочерней политики QoS.

Форма **show** этой команды используется для отображения настройки использования дочерней политики QoS.

22.2.63 policy qos round-robin <имя_политики> class <класс> queue-type <тип>

Указание типа работы с очередью, используемого для класса трафика.

Синтаксис

```
set policy qos round-robin <имя_политики> class <класс> queue-type <тип>
delete policy qos round-robin <имя_политики> class <класс> queue-type
show policy qos round-robin <имя_политики> class <класс> queue-type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      round-robin имя_политики {
         class класс {
            queue-type тип
         }
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики циклического перебора.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4095.

имя_соответствия

Имя правила соответствия для класса.

тип

Используемый метод работы с очередями. Допустимые значения представлены в таблице ниже.

Таблица 192 – Допустимые типы очередей

Значение	Описание
fair-queue	Используется очередь SFQ.
drop-tail	Используется очередь FIFO.
priority	Приоритет в очереди устанавливается по значениям поля DSCP в байте ToS заголовка IP.
random-detect	Используется очередь RED.

Значение по умолчанию

По умолчанию используется тип fair-queue.

Указания по использованию

Эта команда используется для установки типа механизма работы с очередями, используемого в классе трафика.

Форма **set** этой команды используется для указания типа очереди.

Форма **delete** этой команды используется для восстановления типа очереди по умолчанию.

Форма **show** этой команды используется для отображения настройки типа очереди.

22.2.64 policy qos round-robin <имя_политики> default

Определение политики QoS по умолчанию с циклическим перебором.

Синтаксис

```
set policy qos round-robin <имя_политики> default
delete policy qos round-robin <имя_политики> default
show policy qos round-robin <имя_политики> default
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      round-robin имя_политики {
         default {
         }
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики циклического перебора.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения политики циклического перебора по умолчанию. Эта политика будет применена ко всему трафику, не соответствующему никакому другому определенному классу.

Форма **set** этой команды используется для создания узла конфигурации класса по умолчанию.

Форма **delete** этой команды используется для удаления узла конфигурации класса по умолчанию.

Форма **show** этой команды используется для отображения узла конфигурации класса по умолчанию.

22.2.65 policy qos round-robin <имя_политики> default quantum <число_пакетов>

Указание числа пакетов, которые могут быть отправлены за квант планирования.

Синтаксис

```
set policy qos round-robin <имя_политики> default quantum <число_пакетов>
delete policy qos round-robin <имя_политики> default quantum
show policy qos round-robin <имя_политики> default quantum
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        round-robin имя_политики {
            default {
                quantum число_пакетов
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики циклического перебора.

число_пакетов

Необязательный. Число пакетов, которые могут быть отправлены за квант планирования. Значение должно лежать в диапазоне 1-4294967295.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки числа пакетов, которые могут быть отправлены за квант планирования в политике QoS с циклическим перебором.

Форма **set** этой команды используется для указания числа пакетов, которые могут быть отправлены за квант планирования.

Форма **delete** этой команды используется для удаления настройки кванта.

Форма **show** этой команды используется для отображения настройки кванта.

22.2.66 policy qos round-robin <имя_политики> default queue-limit <ограничение>

Указание максимального размера очереди для класса трафика по умолчанию.

Синтаксис

```
set policy qos round-robin <имя_политики> default queue-limit <ограничение>
delete policy qos round-robin <имя_политики> default queue-limit
show policy qos round-robin <имя_политики> default queue-limit
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        round-robin имя_политики {
            default {
                queue-limit ограничение
            }
        }
    }
```

```
}
```

Параметры

имя_политики

Обязательный. Имя политики циклического перебора.

ограничение

Максимальный размер очереди в пакетах. Значение должно лежать в диапазоне 2-4294967295.

Значение по умолчанию

Значение ограничения по умолчанию равно 127.

Указания по использованию

Эта команда используется для установки максимального размера (в пакетах) очереди класса по умолчанию.

Форма **set** этой команды используется для указания ограничения длины очереди.

Форма **delete** этой команды используется для удаления ограничения длины очереди.

Форма **show** этой команды используется для отображения настройки ограничения длины очереди.

22.2.67 policy qos round-robin <имя_политики> default queue-ref <имя_политики>

Указание дочерней политики QoS по умолчанию.

Синтаксис

```
set policy qos round-robin <имя_политики> default queue-ref <имя_политики>
delete policy qos round-robin <имя_политики> default queue-ref
show policy qos round-robin <имя_политики> default queue-ref
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      round-robin имя_политики {
         default {
            queue-ref имя_политики
         }
      }
   }
}
```

Параметры

round-robin *имя_политики*

Обязательный. Имя политики циклического перебора.

queue-ref *имя_политики*

Необязательный. Имя дочерней политики QoS.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки дочерней политики QoS по умолчанию. Данная дочерняя политика будет применяться ко всему трафику, не соответствующему никакому другому определённому классу в рамках указанной политики.

Форма **set** этой команды используется для указания дочерней политики QoS.

Форма **delete** этой команды используется для удаления дочерней политики QoS.

Форма **show** этой команды используется для отображения настройки использования дочерней политики QoS.

22.2.68 policy qos round-robin <имя_политики> default queue-type <тип>

Указание типа работы с очередью, используемого для класса трафика по умолчанию.

Синтаксис

```
set policy qos round-robin <имя_политики> default queue-type <тип>
delete policy qos round-robin <имя_политики> default queue-type
show policy qos round-robin <имя_политики> default queue-type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      round-robin имя_политики {
         default {
            queue-type тип
         }
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики циклического перебора.

тип

Используемый метод работы с очередями. Допустимые значения представлены в таблице ниже.

Таблица 193 – Допустимые типы очередей

Значение	Описание
fair-queue	Используется очередь SFQ.
drop-tail	Используется очередь FIFO.
priority	Приоритет в очереди устанавливается по значениям поля DSCP в байте ToS заголовка IP.
random-detect	Используется очередь RED.

Значение по умолчанию

По умолчанию используется тип fair-queue.

Указания по использованию

Эта команда используется для установки типа механизма работы с очередями, используемого в классе трафика по умолчанию.

Форма **set** этой команды используется для указания типа очереди.

Форма **delete** этой команды используется для восстановления типа очереди по умолчанию.

Форма **show** этой команды используется для отображения настройки типа очереди.

22.2.69 policy qos limiter <имя_политики>

Определение политики QoS с ограничением трафика.

Синтаксис

```
set policy qos limiter <имя_политики>
delete policy qos limiter <имя_политики>
show policy qos limiter <имя_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        limiter имя_политики {
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения политики QoS с ограничением трафика. Политика ограничения трафика применима только к входящему трафику. Имя политики должно быть уникальным и еще не использованным в других командах политик QoS.

Трафик оценивается по правилам соответствия, аналогичным правилам для управления загрузкой исходящего канала. Трафик, не соответствующий никаким правилам, проходит без ограничений. Любой трафик, выходящий за ограничения пропускной способности, отбрасывается.

Форма **set** этой команды используется для создания политики QoS с ограничением трафика.

Форма **delete** этой команды используется для удаления политики QoS с ограничением трафика.

Форма **show** этой команды используется для отображения настройки политики QoS с ограничением трафика.

22.2.70 policy qos limiter <имя_политики> description <описание>

Указание текстового описания политики QoS с ограничением трафика.

Синтаксис

```
set policy qos limiter <имя_политики> description <описание>
delete policy qos limiter <имя_политики> description
show policy qos limiter <имя_политики> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        limiter имя_политики {
```

```
            description описание
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения трафика.

описание

Необязательный. Описание для данной политики ограничения трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указание текстового описания описания политики ограничения трафика.

Форма **set** этой команды используется для указания описания политики ограничения трафика.

Форма **delete** этой команды используется для удаления описания политики ограничения трафика.

Форма **show** этой команды используется для отображения настройки описания политики ограничения трафика.

22.2.71 policy qos limiter <имя_политики> class <класс>

Определение класса трафика для политики QoS с ограничением трафика.

Синтаксис

```
set policy qos limiter <имя_политики> class <класс>
delete policy qos limiter <имя_политики> class <класс>
show policy qos limiter <имя_политики> class <класс>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        limiter имя_политики {
            class класс {
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения трафика.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4090.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения класса трафика в политике QoS с ограничением трафика. Такое определение позволяет группировать пакеты в разные классы трафика, обрабатываемые с разными уровнями обслуживания.

Форма **set** этой команды используется для создания класса трафика в политике QoS с ограничением трафика. До фиксации настройки для класса обязательно должен быть определен параметр bandwidth, в противном случае фиксация завершится сбоем.

Форма **delete** этой команды используется для удаления класса трафика из политики QoS с ограничением трафика.

Форма **show** этой команды используется для отображения настройки класса трафика в политике QoS с ограничением трафика.

22.2.72 policy qos limiter <имя_политики> class <класс> bandwidth <скорость>

Указание ограничения пропускной способности для класса трафика.

Синтаксис

```
set policy qos limiter <имя_политики> class <класс> bandwidth <скорость>
delete policy qos limiter <имя_политики> class <класс> bandwidth
show policy qos limiter <имя_политики> class <класс> bandwidth
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        limiter имя_политики {
            class класс {
                bandwidth скорость
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения трафика.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4090.

скорость

Пропускная способность. Допустимые форматы представлены в таблице ниже.

Таблица 194 – Формат указания пропускной способности

Значение	Описание
<число>	Пропускная способность указанная в килобайтах в секунду.

<число><приставка>	Пропускная способность в указанных единицах измерения. Поддерживаются следующие единицы измерения: **kbit:** килобит в секунду. **mbit:** мегабит в секунду. **gbit:** гигабит в секунду. **kbps:** килобайт в секунду. **mbps:** мегабайт в секунду. **gbps:** гигабайт в секунду.

Значение по умолчанию

Отсутствует. Это значение должно быть установлено обязательно.

Указания по использованию

Эта команда используется для установки ограничения пропускной способности под класс трафика.

Форма **set** этой команды используется для установки пропускной способности, доступной классу трафика.

Форма **delete** этой команды используется для восстановления пропускной способности по умолчанию, доступной классу трафика.

Форма **show** этой команды используется для отображения настройки пропускной способности, доступной классу.

22.2.73 policy qos limiter <имя_политики> class <класс> burst <размер>

Установка размера непрерывной серии пакетов для класса трафика.

Синтаксис

```
set policy qos limiter <имя_политики> class <класс> burst <размер>
delete policy qos limiter <имя_политики> class <класс> burst
show policy qos limiter <имя_политики>class <класс> burst
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        limiter имя_политики {
            class класс {
                burst размер
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения трафика.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4090.

размер

Необязательный. Размер непрерывной серии. Размер непрерывной серии должен находиться в промежутке между 15 КБ и 32 МБ. Допустимые форматы представлены в таблице ниже.

Таблица 195 – Формат указания размера непрерывной серии.

Значение	Описание
<число>	Размер непрерывной серии указанный в байтах.
<число><приставка>	Размер непрерывной серии в указанных единицах измерения. Поддерживаются следующие единицы измерения: **kb:** килобайты. **mb:** мегабайты.

Значение по умолчанию

Длина непрерывной серии составляет 15 килобайт.

Указания по использованию

Эта команда используется для установки размера непрерывной серии в классе трафика. Устанавливается максимальный объем трафика, который может быть передан за один раз.

Форма **set** этой команды используется для указания размера непрерывной серии в классе трафика.

Форма **delete** этой команды используется для восстановления размера непрерывной серии по умолчанию в классе трафика.

Форма **show** этой команды используется для отображения настройки размера непрерывной серии в классе трафика.

22.2.74 policy qos limiter <имя_политики> class <класс> description <описание>

Указание текстового описания для класса трафика.

Синтаксис

```
set policy qos limiter <имя_политики> class <класс> description <описание>
delete policy qos limiter <имя_политики> class <класс> description
show policy qos limiter <имя_политики> class <класс> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      limiter имя_политики {
         class класс {
            description описание
         }
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения трафика.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4090.

описание

Необязательный. Описание для данного класса трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для записи описания класса трафика.

Форма **set** этой команды используется для указания описания.

Форма **delete** этой команды используется для удаления описания.

Форма **show** этой команды используется для отображения настройки описания.

22.2.75 policy qos limiter <имя_политики> class <класс> match <имя_правила>

Определение правила для проверки соответствия классов трафика.

Синтаксис

```
set policy qos limiter <имя_политики> class <класс>match <имя_правила>
delete policy qos limiter <имя_политики> class <класс> match <имя_правила>
show policy qos limiter <имя_политики> class <класс> match <имя_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      limiter имя_политики {
         class класс {
            match имя_правила {
            }
         }
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения трафика.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4090.

имя_правила

Имя правила соответствия для класса.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения правила, устанавливающего условия соответствия для членства в классе трафика.

Форма **set** этой команды используется для создания правила соответствия в классе трафика.

Форма **delete** этой команды используется для удаления узла конфигурации правила соответствия в классе трафика.

Форма **show** этой команды используется для отображения настройки правила соответствия в классе трафика.

22.2.76 policy qos limiter <имя_политики> class <класс> match <имя_правила> description <описание>

Указание текстового описания для правила соответствия.

Синтаксис

```
set policy qos limiter <имя_политики> class <класс> match <имя_правила> description <описание>

delete policy qos limiter <имя_политики> class <класс> match <имя_правила> description

show policy qos limiter <имя_политики> class <класс> match <имя_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        limiter имя_политики {
            class класс {
                match имя_правила {
                    description описание
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения трафика.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4090.

имя_правила

Имя правила соответствия для класса.

описание

Необязательный. Описание для данного соответствия.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для записи описания правила проверки соответствия классов трафика.

Форма **set** этой команды используется для установки описания.

Форма **delete** этой команды используется для удаления описания.

Форма **show** этой команды используется для отображения настройки описания.

22.2.77 policy qos limiter <имя_политики> class <класс> match <имя_правила> ether destination <mac_адрес>

Указание критерия соответствия на основе MAC-адреса получателя.

Синтаксис

```
set policy qos limiter <имя_политики> class <класс> match <имя_правила> ether destination <mac_адрес>

delete policy qos limiter <имя_политики> class <класс> match <имя_правила> ether destination

show policy qos limiter <имя_политики> class <класс> match <имя_правила> ether destination
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        limiter имя_политики {
            class класс {
                match имя_правила {
                    ether {
                        destination mac_адрес
                    }
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения трафика.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4090.

имя_правила

Имя правила соответствия для класса.

mac_адрес

MAC-адрес получателя, на соответствие которому выполняется проверка.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие MAC-адреса получателя.

Указания по использованию

Эта команда используется для определения условия соответствия по MAC-адресу получателя в классе трафика.

ПРИМЕЧАНИЕ Нельзя проверять на соответствие «ip» и «vif» (или «interface»), а также «ip» и «ipv6» одновременно внутри одной и той же настройки ограничения трафика.

Форма **set** этой команды используется для указания получателя, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления получателя в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки получателя в качестве проверяемого условия соответствия.

22.2.78 policy qos limiter <имя_политики> class <класс> match <имя_правила> ether protocol <тип_кадра>

Указание критерия соответствия на основе типа кадра Ethernet.

Синтаксис

```
set policy qos limiter <имя_политики> class <класс> match <имя_правила> ether protocol <тип_кадра>

delete policy qos limiter <имя_политики> class <класс> match <имя_правила> ether protocol

show policy qos limiter <имя_политики> class <класс> match <имя_правила> ether protocol
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        limiter имя_политики {
            class класс {
                match имя_правила {
                    ether {
                        protocol тип_кадра
                    }
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения трафика.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4090.

имя_правила

Имя правила соответствия для класса.

тип_кадра

Тип кадра Ethernet, соответствие которому проверяется, номер типа кадра должен находиться в промежутке от 0 до 65535, либо соответствовать одному из допустимых значений. Допустимые значения представлены в таблице ниже.

Таблица 196 – Допустимые типы кадров ethernet

Значение	Описание
<0-65535>	Номер типа
all	Кадр любого протокола
802.1Q	Кадр протокола 802.1Q VLAN tag
802_2	Кадр протокола 802.2
802_3	Кадр протокола 802.3
aarp	Кадр протокола Appletalk AARP
aoe	Кадр протокола ATA over Ethernet
arp	Кадр протокола Address Resolution Protocol
atalk	Кадр протокола Appletalk DDP
dec	Кадр протокола DEC
ip	Кадр протокола Internet IP (IPv4)
ipv6	Кадр протокола Internet IP (IPv6)
ipx	Кадр протокола Novell Internet Packet Exchange
lat	Кадр протокола DEC LAT
localtalk	Кадр протокола Localtalk
loop	Ethernet loopback
rarp	Кадр протокола Reverse Address Resolution Protocol
snap	Кадр протокола SNAP
x25	Кадр протокола X.25

Значение по умолчанию

Если параметр не установлен, кадры не проверяются на соответствие типа кадра Ethernet.

Указания по использованию

Это команда используется для определения условия соответствия по типу кадра Ethernet в классе трафика.

ПРИМЕЧАНИЕ Нельзя проверять на соответствие «ip» и «vif» (или «interface»), а также «ip» и «ipv6» одновременно внутри одной и той же настройки ограничения трафика.

Форма **set** этой команды используется для указания типа кадра, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления типа кадра в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки типа кадра в качестве проверяемого условия соответствия.

22.2.79 policy qos limiter <имя_политики> class <класс> match <имя_правила> ether source <mac_адрес>

Указание критерия соответствия на основе MAC-адреса отправителя.

Синтаксис

```
set policy qos limiter <имя_политики> class <класс> match <имя_правила> ether source <mac_адрес>

delete policy qos limiter <имя_политики> class <класс> match <имя_правила> ether source

show policy qos limiter <имя_политики> class <класс> match <имя_правила> ether source
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        limiter имя_политики {
            class класс {
                match имя_правила {
                    ether {
                        source mac_адрес
                    }
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения трафика.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4090.

имя_правила

Имя правила соответствия для класса.

mac_адрес

MAC-адрес отправителя, на соответствие которому выполняется проверка.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие MAC-адреса отправителя.

Указания по использованию

Эта команда используется для определения условия соответствия по MAC-адресу отправителя в классе трафика.

ПРИМЕЧАНИЕ Нельзя проверять на соответствие «ip» и «vif» (или «interface»), а также «ip» и «ipv6» одновременно внутри одной и той же настройки ограничения трафика.

Форма **set** этой команды используется для указания отправителя, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления отправителя в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки отправителя в качестве проверяемого условия соответствия.

22.2.80 policy qos limiter <имя_политики> class <класс> match <имя_правила> ip destination

Указание критерия соответствия на основе сведений IP о получателе.

Синтаксис

```
set policy qos limiter <имя_политики> class <класс> match <имя_правила> ip
destination [address <подсеть_ipv4> | port <порт>]
```

```
delete policy qos limiter <имя_политики> class <класс>match <имя_правила> ip destination [address | port]

show policy qos limiter <имя_политики> class <класс> match <имя_правила> ip destination
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      limiter имя_политики {
         class класс {
            match имя_правила {
               ip {
                  destination {
                     address подсеть_ipv4
                     port порт
                  }
               }
            }
         }
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения трафика.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4090.

имя_правила

Имя правила соответствия для класса.

подсеть_ipv4

Необязательный. Адрес подсети IPv4 получателя, на соответствие которому выполняется проверка.

порт

Порт получателя, на соответствие которому выполняется проверка. Порт может быть указан в форме имени строчными буквами (например ssh) или в форме числа.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие сведениям о получателе.

Указания по использованию

Эта команда используется для определения условия соответствия по адресу подсети и/или порту получателя в классе трафика. Можно проверять соответствие для пакетов по адресу подсети IP, порту (портам) получателя или по обоим параметрам вместе.

ПРИМЕЧАНИЕ Нельзя проверять на соответствие «ip» и «vif» (или «interface»), а также «ip» и «ipv6» одновременно внутри одной и той же настройки ограничения трафика.

Форма **set** этой команды используется для указания получателя, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления получателя в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки получателя в качестве проверяемого условия соответствия.

22.2.81 policy qos limiter <имя_политики> class <класс> match <имя_правила> ip dscp <значение>

Указание критерия соответствия на основе значения поля DSCP.

Синтаксис

```
set policy qos limiter <имя_политики> class <класс> match <имя_правила> ip dscp <значение>

delete policy qos limiter <имя_политики> class <класс> match <имя_правила> ip dscp

show policy qos limiter <имя_политики> class <класс> match <имя_правила> ip dscp
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        limiter имя_политики {
            class класс {
                match имя_правила {
                    ip {
                        dscp значение
                    }
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения трафика.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4090.

имя_правила

Имя правила соответствия для класса.

значение

Значение, на соответствие которому выполняется проверка. Это значение сравнивается со значением в поле DSCP байта ToS в заголовке IP.

Таблица 197 – Формат указания параметра значение

Значение	**Описание**
<0-63>	Значение DSCP
default	Соответствует значению DSCP (000000)
EF	Express Forwarding
AFxy	Assured Forwarding, где **x:** Значение в диапазоне 1-4; **y:** Значение в диапазоне 1-3.
CSx	Class Selector, где x – значение в диапазоне 1-7

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие по полю DSCP.

Указания по использованию

Это команда используется для определения условия соответствия по полю DSCP.

Поле DSCP - это 6-битовое поле в байте ToS в заголовке IP. Оно обеспечивает способ отметки пакетов для дальнейшей классификации трафика в классы обслуживания и дальнейшей работы с трафиком наподобие измерения, применения политик и управления загрузкой каналов.

ПРИМЕЧАНИЕ Нельзя проверять на соответствие «ip» и «vif» (или «interface»), а также «ip» и «ipv6» одновременно внутри одной и той же настройки ограничения трафика.

Форма **set** этой команды используется для установки условия соответствия по значению поля DSCP.

Форма **delete** используется для удаления условия соответствия по полю DSCP.

Форма **show** этой команды используется для отображения настройки значения поля DSCP.

22.2.82 policy qos limiter<имя_политики> class <класс> match <имя_правила> ip protocol <протокол>

Указание критерия соответствия на основе протокола IP.

Синтаксис

```
set policy qos limiter <имя_политики> class <класс> match <имя_правила> ip protocol <протокол>

delete policy qos limiter <имя_политики> class <класс> match <имя_правила> ip protocol

show policy qos limiter <имя_политики> class <класс> match <имя_правила> ip protocol
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        limiter имя_политики {
            class класс {
                match имя_правила {
                    ip {
                        protocol протокол
                    }
```

```
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения трафика.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4090.

имя_правила

Имя правила соответствия для класса.

протокол

Имя протокола в текстовом формате (например icmp) или номер, присвоенный организацией IANA, соответствие которому проверяется.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие протоколу IP.

Указания по использованию

Эта команда используется для установки условия соответствия по протоколу в классе трафика.

ПРИМЕЧАНИЕ Нельзя проверять на соответствие «ip» и «vif» (или «interface»), а также «ip» и «ipv6» одновременно внутри одной и той же настройки ограничения трафика.

Форма **set** этой команды используется для установки условия соответствия по протоколу.

Форма **delete** этой команды используется для удаления протокола в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки протокола в качестве проверяемого условия соответствия.

22.2.83 policy qos limiter <имя_политики> class <класс> match <имя_правила> ip source

Указание критерия соответствия на основе сведений IP об отправителе.

Синтаксис

```
set policy qos limiter <имя_политики> class <класс> match <имя_правила> ip source [address <подсеть_ipv4> | port <порт>]

delete policy qos limiter <имя_политики> class <класс> match <имя_правила> ip source [address | port]

show policy qos limiter <имя_политики> class <класс> match <имя_правила> ip source
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        limiter имя_политики {
            class класс {
```

```
                match имя_правила {
                    ip {
                        source {
                            address подсеть_ipv4
                            port порт
                        }
                    }
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения трафика.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4090.

имя_правила

Имя правила соответствия для класса.

подсеть_ipv4

Необязательный. Адрес подсети IPv4 отправителя, на соответствие которому выполняется проверка.

порт

Необязательный. Порт отправителя, на соответствие которому выполняется проверка. Порт может быть указан в форме имени строчными буквами (например ssh) или в форме числа.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие сведениям IP об отправителе.

Указания по использованию

Эта команда используется для определения условия соответствия по адресу подсети и/или порту отправителя в классе трафика. Можно проверять соответствие для пакетов по адресу подсети IP, порту (портам) отправителя или по обоим параметрам вместе.

ПРИМЕЧАНИЕ Нельзя проверять на соответствие «ip» и «vif» (или «interface»), а также «ip» и «ipv6» одновременно внутри одной и той же настройки ограничения трафика.

Форма **set** этой команды используется для указания отправителя, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления отправителя в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки отправителя в качестве проверяемого условия соответствия.

22.2.84 policy qos limiter <имя_политики> class <класс> match <имя_правила> ipv6 destination

Указание критерия соответствия на основе сведений IPv6 о получателе.

Синтаксис

```
set policy qos limiter <имя_политики> class <класс> match <имя_правила> ipv6 destination [address <подсеть_ipv6> | port <порт>]

delete policy qos limiter <имя_политики> class <класс> match <имя_правила> iv6 destination [address | port]

show policy qos limiter <имя_политики> class <класс> match <имя_правила> ipv6 destination
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        limiter имя_политики {
            class класс {
                match имя_правила {
                    ipv6 {
                        destination {
                            address подсеть_ipv6
                            port порт
                        }
                    }
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения трафика.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4090.

имя_правила

Имя правила соответствия для класса.

подсеть_ipv6

Необязательный. Адрес подсети IPv6 получателя, на соответствие которому выполняется проверка.

порт

Порт получателя, на соответствие которому выполняется проверка. Порт может быть указан в форме имени строчными буквами (например ssh) или в форме числа.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие сведениям о получателе.

Указания по использованию

Эта команда используется для определения условия соответствия по адресу подсети и/или порту получателя в классе трафика. Можно проверять соответствие для пакетов по адресу подсети IPv6, порту (портам) получателя или по обоим параметрам вместе.

ПРИМЕЧАНИЕ Нельзя проверять на соответствие «ip» и «vif» (или «interface»), а также «ip» и «ipv6» одновременно внутри одной и той же настройки ограничения трафика.

Форма **set** этой команды используется для указания получателя, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления получателя в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки получателя в качестве проверяемого условия соответствия.

22.2.85 policy qos limiter <имя_политики> class <класс> match <имя_правила> ipv6 dscp <значение>

Указание критерия соответствия на основе значения поля DSCP.

Синтаксис

```
set policy qos limiter <имя_политики> class <класс> match <имя_правила> ipv6 dscp <значение>

delete policy qos limiter <имя_политики> class <класс> match <имя_правила> ipv6 dscp

show policy qos limiter <имя_политики> class <класс> match <имя_правила> ipv6 dscp
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        limiter имя_политики {
            class класс {
                match имя_правила {
                    ipv6 {
                        dscp значение
                    }
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения трафика.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4090.

имя_правила

Имя правила соответствия для класса.

значение

Значение, на соответствие которому выполняется проверка. Это значение сравнивается со значением в поле DSCP байта ToS в заголовке IP.

Таблица 198 – Формат указания параметра значение

Значение	Описание
<0-63>	Значение DSCP
default	Соответствует значению DSCP (000000)
EF	Express Forwarding
AFxy	Assured Forwarding, где **x:** Значение в диапазоне 1-4; **y:** Значение в диапазоне 1-3.
CSx	Class Selector, где x – значение в диапазоне 1-7

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие по полю DSCP.

Указания по использованию

Это команда используется для определения условия соответствия по полю DSCP. Поле DSCP - это 6-битовое поле в байте ToS в заголовке IP. Оно обеспечивает способ отметки пакетов для дальнейшей классификации трафика в классы обслуживания и дальнейшей работы с трафиком наподобие измерения, применения политик и управления загрузкой каналов.

ПРИМЕЧАНИЕ Нельзя проверять на соответствие «ip» и «vif» (или «interface»), а также «ip» и «ipv6» одновременно внутри одной и той же настройки ограничения трафика.

Форма **set** этой команды используется для установки условия соответствия по значению поля DSCP.

Форма **delete** используется для удаления условия соответствия по полю DSCP.

Форма **show** этой команды используется для отображения настройки значения поля DSCP.

22.2.86 policy qos limiter <имя_политики> class <класс> match <имя_правила> ipv6 protocol <протокол>

Указание критерия соответствия на основе протокола IPv6.

Синтаксис

```
set policy qos limiter <имя_политики> class <класс> match <имя_правила> ipv6 protocol <протокол>

delete policy qos limiter <имя_политики> class <класс> match <имя_правила> ipv6 protocol

show policy qos limiter <имя_политики> class <класс> match <имя_правила> ipv6 protocol
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      limiter имя_политики {
         class класс {
            match имя_правила {
```

```
                ipv6 {
                    protocol протокол
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения трафика.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4090.

имя_правила

Имя правила соответствия для класса.

протокол

Имя протокола (например ipv6-icmp) или номер, присвоенный организацией IANA, соответствие которому проверяется.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие протоколу IPv6.

Указания по использованию

Эта команда используется для установки условия соответствия по протоколу в классе трафика.

ПРИМЕЧАНИЕ Нельзя проверять на соответствие «ip» и «vif» (или «interface»), а также «ip» и «ipv6» одновременно внутри одной и той же настройки ограничения трафика.

Форма **set** этой команды используется для установки условия соответствия по протоколу.

Форма **delete** этой команды используется для удаления протокола в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки протокола в качестве проверяемого условия соответствия.

22.2.87 policy qos limiter <имя_политики> class <класс> match <имя_правила> ipv6 source

Указание критерия соответствия на основе сведений IPv6 об отправителе.

Синтаксис

```
set policy qos limiter <имя_политики> class <класс> match <имя_правила> ipv6 source [address <подсеть_ipv6> | port <порт>]

delete policy qos limiter <имя_политики> class <класс> match <имя_правила> ipv6 source [address | port]

show policy qos limiter <имя_политики> class <класс> match <имя_правила> ipv6 source
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
```

```
qos {
    limiter имя_политики {
        class класс {
            match имя_правила {
                ipv6 {
                    source {
                        address подсеть_ipv4
                        port порт
                    }
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения трафика.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4090.

имя_правила

Имя правила соответствия для класса.

подсеть_ipv6

Необязательный. Адрес подсети IPv6 отправителя, на соответствие которому выполняется проверка.

порт

Необязательный. Порт отправителя, на соответствие которому выполняется проверка. Порт может быть указан в форме имени строчными буквами (например ssh) или в форме числа.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие сведениям IP об отправителе.

Указания по использованию

Эта команда используется для определения условия соответствия по адресу подсети и/или порту отправителя в классе трафика. Можно проверять соответствие для пакетов по адресу подсети IPv6, порту (портам) отправителя или по обоим параметрам вместе.

ПРИМЕЧАНИЕ Нельзя проверять на соответствие «ip» и «vif» (или «interface»), а также «ip» и «ipv6» одновременно внутри одной и той же настройки ограничения трафика.

Форма **set** этой команды используется для указания отправителя, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления отправителя в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки отправителя в качестве проверяемого условия соответствия.

22.2.88 policy qos limiter <имя_политики> class <класс> match <имя_правила> vif <идентификатор_vlan>

Указание критерия соответствия на основе идентификатора VLAN.

Синтаксис

```
set policy qos limiter <имя_политики> class <класс> match <имя_правила> vif <идентификатор_vlan>

delete policy qos limiter <имя_политики> class <класс> match <имя_правила> vif

show policy qos limiter <имя_политики> class <класс> match <имя_правила> vif
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        limiter имя_политики {
            class класс {
                match имя_правила {
                    vif идентификатор_vlan
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения трафика.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4090.

имя_правила

Имя правила соответствия для класса.

идентификатор_vlan

Идентификатор VLAN, соответствие которому проверяется. Значение должно находиться в диапазоне от 1 до 4094.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие идентификатору VLAN.

Указания по использованию

Это команда используется для определения условия соответствия по идентификатору VLAN в классе трафика.

ПРИМЕЧАНИЕ Нельзя проверять на соответствие «ip» и «vif» (или «interface»), а также «ip» и «ipv6» одновременно внутри одной и той же настройки ограничения трафика.

Форма **set** этой команды используется для указания идентификатора VLAN, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления идентификатора VLAN в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки идентификатора VLAN в качестве проверяемого условия соответствия.

22.2.89 policy qos limiter <имя_политики> class <класс> priority <приоритет>

Указание порядка обработки правил соответствия.

Синтаксис

```
set policy qos limiter <имя_политики> class <класс> priority <приоритет>
delete policy qos limiter <имя_политики> class <класс> priority
show policy qos limiter <имя_политики> class <класс> priority
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      limiter имя_политики {
         class класс {
            priority приоритет
         }
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики ограничения трафика.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 1 до 4090.

приоритет

Необязательный. Приоритет проверки правил соответствия. Чем больше значение, тем ниже приоритет. Значение должно лежать в диапазоне 0-20.

Значение по умолчанию

Классам трафика назначается приоритет 20.

Указания по использованию

Эта команда используется для установки приоритета обработки правил совпадения.

Форма **set** этой команды используется для указания приоритета класса трафика.

Форма **delete** используется для восстановления приоритета по умолчанию данного класса трафика.

Форма **show** этой команды используется для отображения настройки приоритета класса трафика.

22.2.90 policy qos shaper <имя_политики>

Определение политики QoS с управлением загрузкой канала.

Синтаксис

```
set policy qos shaper <имя_политики>
delete policy qos shaper <имя_политики>
```

```
show policy qos shaper <имя_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
       shaper имя_политики {
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения политики QoS с управлением загрузкой канала. Политика управления загрузкой канала применима только к исходящему трафику. Имя политики должно быть уникальным и еще не использованным в других командах политик QoS.

В Numa Edge используется вариант алгоритма "маркерного ведра" для управления загрузкой канала. В алгоритме "маркерного ведра" устанавливается ограничение на среднюю скорость передачи трафика, однако разрешаются контролируемые серии пакетов в сети. Алгоритм "маркерного ведра" предоставляет возможность контролировать пропускную способность под VoIP или ограничивать потребление пропускной способности для пиринговых приложений.

Основу алгоритма "маркерного ведра" составляет буфер ("ведро"), постоянно заполняющийся маркерами (token) с заданной скоростью. Каждый прибывающий маркер сопоставляется с одним пакетом данных из очереди, после чего удаляется. Возможны 3 различные ситуации:

- Данные прибывают со скоростью равной скорости входящих маркеров. В этом случае каждый пакет имеет соответствующий маркер и проходит очередь без задержки;
- Данные прибывают со скоростью меньшей скорости поступления маркеров. В этом случае лишь часть существующих маркеров будет уничтожаться, поэтому они станут накапливаться до размера буфера. Далее накопленные маркеры могут использоваться при "всплесках" (burst) для передачи данных со скоростью, превышающей скорость пребывающих маркеров;
- Данные прибывают быстрее, чем маркеры. Это означает, что в буфере не останется маркеров, то есть придется приостановить передачу данных. Если пакеты продолжают поступать, они начинают уничтожаться. Это позволяет административно ограничивать доступную полосу пропускания.

Различие между алгоритмами управления загрузкой канала и циклического перебора состоит в том, что первый ограничивает использование пропускной способности классом и затем распределяет любую оставшуюся пропускную способность. Напротив, при циклическом переборе делается попытка разделить пропускную способность между определенными классами.

Форма **set** этой команды используется для создания политики QoS с управлением загрузкой канала.

Форма **delete** этой команды используется для удаления политики QoS с управлением загрузкой канала.

Форма **show** этой команды используется для отображения настройки политики QoS с управлением загрузкой канала.

22.2.91 policy qos shaper <имя_политики> bandwidth <скорость>

Указание пропускной способности, доступной для всего суммарного трафика, ограничиваемого данной политикой.

Синтаксис

```
set policy qos shaper <имя_политики> bandwidth <скорость>
delete policy qos shaper <имя_политики> bandwidth
show policy qos shaper <имя_политики> bandwidth
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      shaper имя_политики {
         bandwidth скорость
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

скорость

Пропускная способность. Допустимые форматы представлены в таблице ниже.

Таблица 199 – Формат указания пропускной способности

Значение	Описание
auto	Пропускная способность основана на скорости интерфейса
<число>	Пропускная способность указанная в килобайтах в секунду.
<число><приставка>	Пропускная способность в указанных единицах измерения. Поддерживаются следующие единицы измерения: **kbit:** килобит в секунду. **mbit:** мегабит в секунду. **gbit:** гигабит в секунду. **kbps:** килобайт в секунду. **mbps:** мегабайт в секунду. **gbps:** гигабайт в секунду.

Значение по умолчанию

По умолчанию используется значение **auto**.

Указания по использованию

Эта команда используется для установки ограничений на пропускную способность в политике QoS управления загрузкой канала. Данный параметр описывает максимальную пропускную способность, доступную всем классам.

Форма **set** этой команды используется для указания ограничений пропускной способности для политики.

Форма **delete** этой команды используется для восстановления ограничений пропускной способности по умолчанию.

Форма **show** этой команды используется для отображения настройки пропускной способности, выделенной политике.

22.2.92 policy qos shaper <имя_политики> description <описание>

Указание текстового описания политики QoS с управлением загрузкой канала.

Синтаксис

```
set policy qos shaper <имя_политики> description <описание>
delete policy qos shaper <имя_политики> description
show policy qos shaper <имя_политики> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      shaper имя_политики {
         description описание
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

описание

Необязательный. Описание для данной политики управления загрузкой канала.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для записи описания политики управления загрузкой канала.

Форма **set** этой команды используется для указания описания политики управления загрузкой канала.

Форма **delete** этой команды используется для удаления описания политики управления загрузкой канала.

Форма **show** этой команды используется для отображения настройки описания политики управления загрузкой канала.

22.2.93 policy qos shaper <имя_политики> class <класс>

Определение класса трафика для политики QoS с управлением загрузкой канала.

Синтаксис

```
set policy qos shaper <имя_политики> class <класс>
delete policy qos shaper <имя_политики> class <класс>
show policy qos shaper <имя_политики> class <класс>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      shaper имя_политики {
         class класс {
         }
      }
```

```
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 2 до 4095.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения класса трафика в политике QoS с управлением загрузкой канала. Такое определение позволяет группировать пакеты в разные классы трафика, обрабатываемые с разными уровнями обслуживания.

Форма **set** этой команды используется для создания класса трафика в политике QoS с управлением загрузкой канала.

Форма **delete** этой команды используется для удаления класса трафика из политики QoS с управлением загрузкой канала.

Форма **show** этой команды используется для отображения настройки класса трафика в политике QoS с управлением загрузкой канала.

22.2.94 policy qos shaper <имя_политики> class <класс> bandwidth <скорость>

Указание базовой гарантированной пропускной способности для класса трафика.

Синтаксис

```
set policy qos shaper <имя_политики> class <класс> bandwidth <скорость>
delete policy qos shaper <имя_политики> class <класс> bandwidth
show policy qos shaper <имя_политики> class <класс> bandwidth
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        shaper имя_политики {
            class класс {
                bandwidth скорость
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 2 до 4095.

скорость

Пропускная способность. Допустимые форматы представлены в таблице ниже.

Таблица 200 – Формат указания пропускной способности

Значение	Описание
<число>	Пропускная способность указанная в килобайтах в секунду.
<число>%%	Пропускная способность указанная в процентах от общей.
<число><приставка>	Пропускная способность в указанных единицах измерения. Поддерживаются следующие единицы измерения: **kbit:** килобит в секунду. **mbit:** мегабит в секунду. **gbit:** гигабит в секунду. **kbps:** килобайт в секунду. **mbps:** мегабайт в секунду. **gbps:** гигабайт в секунду.

Значение по умолчанию

Доступно для использования 100% пропускной способности.

Указания по использованию

Эта команда используется для установки гарантированной пропускной способности под класс трафика.

Форма **set** этой команды используется для установки пропускной способности, доступной классу трафика.

Форма **delete** этой команды используется для восстановления пропускной способности по умолчанию, доступной классу трафика.

Форма **show** этой команды используется для отображения настройки пропускной способности, доступной классу.

22.2.95 policy qos shaper <имя_политики> class <класс> burst <размер>

Установка размера непрерывной серии пакетов для класса трафика.

Синтаксис

```
set policy qos shaper <имя_политики> class <класс> burst <размер>
delete policy qos shaper <имя_политики> class <класс> burst
show policy qos shaper <имя_политики> class <класс> burst
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      shaper имя_политики {
         class класс {
            burst размер
         }
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 2 до 4095.

размер

Необязательный. Размер непрерывной серии. Размер непрерывной серии должен находиться в промежутке между 15 КБ и 32 МБ. Допустимые форматы представлены в таблице ниже.

Таблица 201 – Формат указания размера непрерывной серии.

Значение	**Описание**
<число>	Размер непрерывной серии указанный в байтах.
<число><приставка>	Размер непрерывной серии в указанных единицах измерения. Поддерживаются следующие единицы измерения: **kb:** килобайты. **mb:** мегабайты.

Значение по умолчанию

Длина серии составляет 15 килобайт.

Указания по использованию

Эта команда используется для установки размера непрерывной серии в классе трафика. Устанавливается максимальный объем трафика, который может быть передан за один раз.

Форма **set** этой команды используется для указания размера непрерывной серии в классе трафика.

Форма **delete** этой команды используется для восстановления размера непрерывной серии по умолчанию в классе трафика.

Форма **show** этой команды используется для отображения настройки размера непрерывной серии в классе трафика.

22.2.96 policy qos shaper <имя_политики> default ceiling <скорость>

Установка верхней границы пропускной способности для класса трафика.

Синтаксис

```
set policy qos shaper <имя_политики> class <класс> ceiling <скорость>
delete policy qos shaper <имя_политики> class <класс> ceiling
show policy qos shaper <имя_политики> class <класс> ceiling
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        shaper имя_политики {
            class класс {
                ceiling скорость
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

класс

Обязательный. Идентификатор класса. Значение должно находиться в диапазоне от 2 до 4095.

скорость

Пропускная способность. Допустимые форматы представлены в таблице ниже.

Таблица 202 – Формат указания пропускной способности

Значение	Описание
<число>	Пропускная способность указанная в килобайтах в секунду.
<число>%%	Пропускная способность указанная в процентах от общей.
<число><приставка>	Пропускная способность в указанных единицах измерения. Поддерживаются следующие единицы измерения: **kbit:** килобит в секунду. **mbit:** мегабит в секунду. **gbit:** гигабит в секунду. **kbps:** килобайт в секунду. **mbps:** мегабайт в секунду. **gbps:** гигабайт в секунду.

Значение по умолчанию

Значением по умолчанию является пропускная способность, указанная для класса.

Указания по использованию

Эта команда используется для установки максимальной пропускной способности, которую класс трафика может использовать при наличии излишков пропускной способности.

Форма **set** этой команды используется для установки верхнего ограничения пропускной способности, доступной классу трафика.

Форма **delete** этой команды используется для восстановления верхнего ограничения пропускной способности по умолчанию, доступной классу трафика.

Форма **show** этой команды используется для отображения настройки верхнего ограничения пропускной способности, доступной классу трафика.

22.2.97 policy qos shaper <имя_политики> class <класс> description <описание>

Указание текстового описания для класса трафика.

Синтаксис

```
set policy qos shaper <имя_политики> class <класс> description <описание>
delete policy qos shaper <имя_политики> class <класс> description
show policy qos shaper <имя_политики> class <класс> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        shaper имя_политики {
            class класс {
                description описание
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 2 до 4095.

описание

Необязательный. Описание для данного класса трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для записи описания класса трафика.

Форма **set** этой команды используется для указания описания.

Форма **delete** этой команды используется для удаления описания.

Форма **show** этой команды используется для отображения настройки описания.

22.2.98 policy qos shaper <имя_политики> class <класс> match <имя_правила>

Определение правила для проверки соответствия классов трафика.

Синтаксис

```
set policy qos shaper <имя_политики> class <класс> match <имя_правила>
delete policy qos shaper <имя_политики> class <класс> match <имя_правила>
show policy qos shaper <имя_политики> class <класс> match <имя_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      shaper имя_политики {
         class класс {
            match имя_правила {
            }
         }
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 2 до 4095.

имя_правила

Имя правила соответствия для класса в текстовом формате.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения правила, устанавливающего условия соответствия для членства в классе трафика.

Форма **set** этой команды используется для создания правила соответствия в классе трафика.

Форма **delete** этой команды используется для удаления узла конфигурации правила соответствия в классе трафика.

Форма **show** этой команды используется для отображения настройки правила соответствия в классе трафика.

22.2.99 policy qos shaper <имя_политики> class <класс> match <имя_правила> description <описание>

Указание текстового описания для правила соответствия.

Синтаксис

```
set policy qos shaper <имя_политики> class <класс> match <имя_правила> description <описание>

delete policy qos shaper <имя_политики> class <класс> match <имя_правила> description

show policy qos shaper <имя_политики> class <класс> match <имя_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        shaper имя_политики {
            class класс {
                match имя_правила {
                    description описание
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 2 до 4095.

имя_правила

Имя правила соответствия для класса.

описание

Описание для данного соответствия.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для записи описания правила проверки соответствия классов трафика.

Форма **set** этой команды используется для установки описания.

Форма **delete** этой команды используется для удаления описания.

Форма **show** этой команды используется для отображения настройки описания.

22.2.100 policy qos shaper <имя_политики> class <класс> match <имя_правила> ether destination <mac_адрес>

Указание критерия соответствия на основе MAC-адреса получателя.

Синтаксис

```
set policy qos shaper <имя_политики> class <класс> match <имя_правила> ether destination <mac_адрес>

delete policy qos shaper <имя_политики> class <класс> match <имя_правила> ether destination

show policy qos shaper <имя_политики> class <класс>match <имя_правила> ether destination
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        shaper имя_политики {
            class класс {
                match имя_правила {
                    ether {
                        destination mac_адрес
                    }
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 2 до 4095.

имя_соответствия

Необязательный. Имя правила соответствия для класса.

mac_адрес

Необязательный. MAC-адрес получателя, на соответствие которому выполняется проверка.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие MAC-адреса получателя.

Указания по использованию

Эта команда используется для определения условия соответствия по MAC-адресу получателя в классе трафика.

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для указания получателя, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления получателя в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки получателя в качестве проверяемого условия соответствия.

22.2.101 policy qos shaper <имя_политики> class <класс> match <имя_правила> ether protocol <тип_кадра>

Указание критерия соответствия на основе типа кадра Ethernet.

Синтаксис

```
set policy qos shaper <имя_политики> class <класс> match <имя_правила> ether protocol <тип_кадра>

delete policy qos shaper <имя_политики> class <класс> match <имя_правила> ether protocol

show policy qos shaper <имя_политики> class <класс> match <имя_правила> ether protocol
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        shaper имя_политики {
            class класс {
                match имя_правила {
                    ether {
                        protocol тип_кадра
                    }
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 2 до 4095.

имя_правила

Имя правила соответствия для класса.

тип_кадра

Тип кадра Ethernet, соответствие которому проверяется, номер типа кадра должен находиться в промежутке от 0 до 65535, либо соответствовать одному из допустимых значений. Допустимые значения представлены в таблице ниже.

Таблица 203 – Допустимые типы кадров ethernet

Значение	**Описание**
<0-65535>	Номер типа
all	Кадр любого протокола
802.1Q	Кадр протокола 802.1Q VLAN tag
802_2	Кадр протокола 802.2
802_3	Кадр протокола 802.3
aarp	Кадр протокола Appletalk AARP
aoe	Кадр протокола ATA over Ethernet
arp	Кадр протокола Address Resolution Protocol
atalk	Кадр протокола Appletalk DDP
dec	Кадр протокола DEC
ip	Кадр протокола Internet IP (IPv4)
ipv6	Кадр протокола Internet IP (IPv6)
ipx	Кадр протокола Novell Internet Packet Exchange
lat	Кадр протокола DEC LAT
localtalk	Кадр протокола Localtalk
loop	Ethernet loopback
rarp	Кадр протокола Reverse Address Resolution Protocol
snap	Кадр протокола SNAP
x25	Кадр протокола X.25

Значение по умолчанию

Если параметр не установлен, кадры не проверяются на соответствие типа кадра Ethernet.

Указания по использованию

Это команда используется для определения условия соответствия по типу кадра Ethernet в классе трафика.

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для указания типа кадра, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления типа кадра в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки типа кадра в качестве проверяемого условия соответствия.

22.2.102 policy qos shaper <имя_политики> class <класс> match <имя_правила> ether source <mac_адрес>

Указание критерия соответствия на основе MAC-адреса отправителя.

Синтаксис

```
set policy qos shaper <имя_политики> class <класс> match <имя_правила> ether source <mac_адрес>

delete policy qos shaper <имя_политики> class <класс> match <имя_правила> ether source

show policy qos shaper <имя_политики> class <класс> match <имя_правила> ether source
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        shaper имя_политики {
            class класс {
                match имя_правила {
                    ether {
                        source mac_адрес
                    }
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 2 до 4095.

имя_соответствия

Имя правила соответствия для класса.

mac_адрес

MAC-адрес отправителя, на соответствие которому выполняется проверка.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие MAC-адреса отправителя.

Указания по использованию

Эта команда используется для определения условия соответствия по MAC-адресу отправителя в классе трафика.

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для указания отправителя, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления отправителя в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки отправителя в качестве проверяемого условия соответствия.

22.2.103 policy qos shaper <имя_политики> class <класс> match <имя_правила> filter <имя_фильтра>

Указание критерия соответствия на основе определённого фильтра IPv4-трафика.

Синтаксис

```
set policy qos shaper <имя_политики> class <класс> match <имя_правила> filter <имя_фильтра>

delete policy qos shaper <имя_политики> class <класс> match <имя_правила> filter <имя_фильтра>

show policy qos shaper <имя_политики> class <класс> match <имя_правила> filter
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        shaper имя_политики {
            class класс {
                match имя_правила {
                    filter имя_фильтра
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 2 до 4095.

имя_соответствия

Имя правила соответствия для класса.

имя_фильтра

Необязательный. Имя определённого фильтра IPv4-трафика.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие сведениям о получателе.

Указания по использованию

Эта команда используется для определения условия соответствия на основе определённого фильтра IPv4-трафика в классе трафика.

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для указания фильтра трафика, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления фильтра трафика в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки фильтра трафика в качестве проверяемого условия соответствия.

22.2.104 policy qos shaper <имя_политики> class <класс> match <имя_правила> filter-ipv6 <имя_фильтра>

Указание критерия соответствия на основе определённого фильтра IPv6-трафика.

Синтаксис

```
set policy qos shaper <имя_политики> class <класс> match <имя_правила> filter-ipv6 <имя_фильтра>

delete policy qos shaper <имя_политики> class <класс> match <имя_правила> filter-ipv6 <имя_фильтра>

show policy qos shaper <имя_политики> class <класс> match <имя_правила> filter-ipv6
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        shaper имя_политики {
            class класс {
                match имя_правила {
                    filter-ipv6 имя_фильтра
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 2 до 4095.

имя_соответствия

Имя правила соответствия для класса.

имя_фильтра

Необязательный. Имя определённого фильтра IPv6-трафика.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие сведениям о получателе.

Указания по использованию

Эта команда используется для определения условия соответствия на основе определённого фильтра IPv6-трафика в классе трафика.

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для указания фильтра трафика, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления фильтра трафика в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки фильтра трафика в качестве проверяемого условия соответствия.ъ

22.2.105 policy qos shaper <имя_политики> class <класс> match <имя_правила> interface <интерфейс>

Указание критерия соответствия на основе входного интерфейса пакетов.

Синтаксис

```
set policy qos shaper <имя_политики> class <класс> match <имя_правила> interface <интерфейс>

delete policy qos shaper <имя_политики> class <класс> match <имя_правила> interface

show policy qos shaper <имя_политики> class <класс> match <имя_правила> interface
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        shaper имя_политики {
            class класс {
                match имя_правила {
                    interface интерфейс
                }
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 2 до 4095.

имя_соответствия

Имя правила соответствия для класса.

интерфейс

Имя интерфейса Ethernet, на соответствие которому выполняется проверка. С указанным значением будет сравниваться входной интерфейс пакета.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки условия соответствия по входному интерфейсу в классе трафика. Если входящие пакеты попадают в систему через интерфейс, указанный данной командой, то трафик будет членом данного класса трафика (при условии, что другие условия соответствия удовлетворяются).

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для указания входного интерфейса пакетов.

Форма **delete** этой команды используется для удаления соответствия по интерфейсу.

Форма **show** этой команды используется для отображения настройки соответствия по интерфейсу.

22.2.106 policy qos shaper <имя_политики> class <класс> match <имя_правила> vif <идентификатор_vlan>

Указание критерия соответствия на основе идентификатора VLAN.

Синтаксис

```
set policy qos shaper <имя_политики> class <класс> match <имя_правила> vif <идентификатор_vlan>
delete policy qos shaper <имя_политики> class <класс> match <имя_правила> vif
show policy qos shaper <имя_политики> class <класс> match <имя_правила> vif
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        shaper имя_политики {
            class класс {
                match имя_правила {
                    vif идентификатор_vlan
                }
            }
```

```
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 2 до 4095.

имя_соответствия

Имя правила соответствия для класса.

идентификатор_vlan

Идентификатор VLAN, соответствие которому проверяется. Значение должно находиться в диапазоне от 1 до 4094.

Значение по умолчанию

Если параметр не установлен, пакеты не проверяются на соответствие идентификатору VLAN.

Указания по использованию

Это команда используется для определения условия соответствия по идентификатору VLAN в классе трафика.

ПРИМЕЧАНИЕ В рамках одного правила соответствия (match), невозможно одновременное использование выборки трафика по фильтру («filter»/«filter-ipv6») и по какому-либо другому критерию («ether»/«interface»/«vif»). Также невозможно одновременное использование критериев «ether» и «interface» (или «vif»). При этом, возможно одновременное использование критериев «interface» и «vif».

Форма **set** этой команды используется для указания идентификатора VLAN, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления идентификатора VLAN в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки идентификатора VLAN в качестве проверяемого условия соответствия.

22.2.107 policy qos shaper <имя_политики> class <класс> priority <приоритет>

Указание приоритета класса трафика при выделении дополнительной пропускной способности.

Синтаксис

```
set policy qos shaper <имя_политики> class <класс> priority <приоритет>
delete policy qos shaper <имя_политики> class <класс> priority
show policy qos shaper <имя_политики> class <класс> priority
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        shaper имя_политики {
            class класс {
                priority приоритет
            }
```

```
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 2 до 4095.

приоритет

Приоритет, в соответствии с которым данному классу будет выделяться дополнительная пропускная способность. Чем меньше значение, тем ниже приоритет. Значение должно находиться в диапазоне от 0 до 7.

Значение по умолчанию

Классам трафика назначается приоритет 0.

Указания по использованию

Эта команда используется для назначения приоритета, по которому классу трафика выделяется дополнительная пропускная способность, когда она имеется.

Форма **set** этой команды используется для указания приоритета класса трафика.

Форма **delete** используется для восстановления приоритета по умолчанию данного класса трафика.

Форма **show** этой команды используется для отображения настройки приотритета класса трафика.

22.2.108 policy qos shaper <имя_политики> class <класс> queue-limit <ограничение>

Указание максимального размера очереди для класса трафика.

Синтаксис

```
set policy qos shaper <имя_политики> class <класс> queue-limit <ограничение>
delete policy qos shaper <имя_политики> class <класс> queue-limit
show policy qos shaper <имя_политики> class <класс> queue-limit
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        shaper имя_политики {
            class класс {
                queue-limit ограничение
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 2 до 4095.

ограничение

Максимальный размер очереди в пакетах. Значение должно лежать в диапазоне 1-4294967295.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки максимального размера очереди (в пакетах) в классе трафика.

Форма **set** этой команды используется для указания ограничения длины очереди.

Форма **delete** этой команды используется для удаления ограничения длины очереди.

Форма **show** этой команды используется для отображения настройки ограничения длины очереди.

22.2.109 policy qos shaper <имя_политики> class <класс> queue-ref <имя_политики>

Указание дочерней политики QoS для данного класса трафика.

Синтаксис

```
set policy qos shaper <имя_политики> class <класс> queue-ref <имя_политики>
delete policy qos shaper <имя_политики> class <класс> queue-ref <имя_политики>
show policy qos shaper <имя_политики> class <класс> queue-ref
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      shaper имя_политики {
         class класс {
            queue-ref имя_политики
         }
      }
   }
}
```

Параметры

shaper *имя_политики*

Обязательный. Имя политики управления загрузкой канала.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 2 до 4095.

queue-ref *имя_политики*

Необязательный. Имя дочерней политики QoS.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки дочерней политики QoS. Данная дочерняя политика будет применяться к трафику, попавшему в указанный класс.

Форма **set** этой команды используется для указания дочерней политики QoS.

Форма **delete** этой команды используется для удаления дочерней политики QoS.

Форма **show** этой команды используется для отображения настройки использования дочерней политики QoS.

22.2.110 policy qos shaper <имя_политики> class <класс> queue-type <тип>

Указание типа работы с очередью, используемого для класса трафика.

Синтаксис

```
set policy qos shaper <имя_политики> class <класс> queue-type <тип>
delete policy qos shaper <имя_политики> class <класс> queue-type
show policy qos shaper <имя_политики> class <класс>queue-type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      shaper имя_политики {
         class класс {
            queue-type тип
         }
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

класс

Обязательный. Идентификатор класса. Значение должно находится в диапазоне от 2 до 4095.

тип

Используемый метод работы с очередями. Допустимые значения представлены в таблице ниже.

Таблица 204 – Допустимые типы очередей

Значение	Описание
fair-queue	Используется очередь SFQ.
drop-tail	Используется очередь FIFO.
priority	Приоритет в очереди устанавливается по значениям поля DSCP в байте ToS заголовка IP.
random-detect	Используется очередь RED.

Значение по умолчанию

По умолчанию используется тип fair-queue.

Указания по использованию

Эта команда используется для установки типа механизма работы с очередями, используемого в классе трафика.

Форма **set** этой команды используется для указания типа очереди.

Форма **delete** этой команды используется для восстановления типа очереди по умолчанию.

Форма **show** этой команды используется для отображения настройки типа очереди.

22.2.111 policy qos shaper <имя_политики> default

Определение политики QoS по умолчанию с управлением загрузкой канала.

Синтаксис

```
set policy qos shaper <имя_политики> default
delete policy qos shaper <имя_политики> default
show policy qos shaper <имя_политики> default
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        shaper имя_политики {
            default {
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения политики управления загрузкой канала по умолчанию. Эта политика будет применена ко всему трафику, не соответствующему никакому другому определенному классу.

Форма **set** этой команды используется для создания узла конфигурации класса по умолчанию.

Форма **delete** этой команды используется для удаления узла конфигурации класса по умолчанию.

Форма **show** этой команды используется для отображения узла конфигурации класса по умолчанию.

22.2.112 policy qos shaper <имя_политики> default bandwidth <скорость>

Указание базовой гарантированной пропускной способности для класса трафика по умолчанию.

Синтаксис

```
set policy qos shaper <имя_политики> default bandwidth <скорость>
delete policy qos shaper <имя_политики> default
bandwidth show policy qos shaper <имя_политики> default bandwidth
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        shaper имя_политики {
            default {
```

```
            bandwidth скорость
        }
    }
  }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

скорость

Пропускная способность. Допустимые форматы представлены в таблице ниже.

Таблица 205 – Формат указания пропускной способности

Значение	Описание
<число>	Пропускная способность указанная в килобайтах в секунду.
<число>%%	Пропускная способность указанная в процентах от общей.
<число><приставка>	Пропускная способность в указанных единицах измерения. Поддерживаются следующие единицы измерения: **kbit:** килобит в секунду. **mbit:** мегабит в секунду. **gbit:** гигабит в секунду. **kbps:** килобайт в секунду. **mbps:** мегабайт в секунду. **gbps:** гигабайт в секунду.

Значение по умолчанию

Доступно для использования 100% пропускной способности.

Указания по использованию

Эта команда используется для установки базового уровня гарантированной пропускной способности, доступной классу трафика по умолчанию.

Форма **set** этой команды используется для установки пропускной способности, доступной классу трафика по умолчанию.

Форма **delete** этой команды используется для восстановления пропускной способности по умолчанию, доступной классу трафика по умолчанию.

Форма **show** этой команды используется для отображения настройки пропускной способности, доступной классу трафика по умолчанию.

22.2.113 policy qos shaper <имя_политики> default burst

Установка размера непрерывной серии пакетов для класса трафика по умолчанию.

Синтаксис

```
set policy qos shaper <имя_политики> default burst <размер>
delete policy qos shaper <имя_политики> default burst
show policy qos shaper <имя_политики> default burst
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      shaper имя_политики {
```

```
            default {
               burst размер
            }
         }
      }
   }
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

размер

Необязательный. Размер непрерывной серии. Размер непрерывной серии должен находиться в промежутке между 15 КБ и 32 МБ. Допустимые форматы представлены в таблице ниже.

Таблица 206 – Формат указания размера непрерывной серии.

Значение	Описание
<число>	Размер непрерывной серии указанный в байтах.
<число><приставка>	Размер непрерывной серии в указанных единицах измерения. Поддерживаются следующие единицы измерения: **kb:** килобайты. **mb:** мегабайты.

Значение по умолчанию

Размер непрерывной серии равен 15 килобайт.

Указания по использованию

Эта команда используется для установки размера непрерывной серии в классе трафика по умолчанию. Устанавливается максимальный объем трафика, который может быть передан за один раз.

Форма **set** этой команды используется для указания размера непрерывной серии в классе трафика по умолчанию.

Форма **delete** этой команды используется для восстановления размера серии по умолчанию в классе трафика по умолчанию.

Форма **show** этой команды используется для отображения настройки размера непрерывной серии в классе трафика по умолчанию.

22.2.114 policy qos shaper <имя_политики> default ceiling <скорость>

Установка верхней границы пропускной способности для класса трафика по умолчанию.

Синтаксис

```
set policy qos shaper <имя_политики> default ceiling <скорость>
delete policy qos shaper <имя_политики> default ceiling
show policy qos shaper <имя_политики> default ceiling
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      shaper имя_политики {
         default {
            ceiling скорость
```

```
            }
        }
    }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

скорость

Пропускная способность. Допустимые форматы представлены в таблице ниже.

Таблица 207 – Формат указания пропускной способности

Значение	Описание
<число>	Пропускная способность указанная в килобайтах в секунду.
<число>%%	Пропускная способность указанная в процентах от общей.
<число><приставка>	Пропускная способность в указанных единицах измерения. Поддерживаются следующие единицы измерения: **kbit:** килобит в секунду. **mbit:** мегабит в секунду. **gbit:** гигабит в секунду. **kbps:** килобайт в секунду. **mbps:** мегабайт в секунду. **gbps:** гигабайт в секунду.

Значение по умолчанию

По умолчанию доступна вся пропускная способность.

Указания по использованию

Эта команда используется для установки максимальной пропускной способности, которую класс трафика по умолчанию может использовать при наличии излишков пропускной способности.

Форма **set** этой команды используется для установки верхнего ограничения пропускной способности, доступной классу трафика по умолчанию.

Форма **delete** этой команды используется для восстановления верхнего ограничения пропускной способности по умолчанию, доступной классу трафика по умолчанию.

Форма **show** этой команды используется для отображения настройки верхнего ограничения пропускной способности, доступной классу трафика по умолчанию.

22.2.115 policy qos shaper <имя_политики> default priority <приоритет>

Указание приоритета класса трафика по умолчанию при выделении дополнительной пропускной способности.

Синтаксис

```
set policy qos shaper <имя_политики> default priority <приоритет>
delete policy qos shaper <имя_политики> default priority
show policy qos shaper <имя_политики> default priority
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    qos {
        shaper имя_политики {
```

```
            default {
               priority приоритет
            }
         }
      }
   }
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

приоритет

Приоритет, в соответствии с которым данному классу будет выделяться дополнительная пропускная способность. Чем меньше значение, тем ниже приоритет. Значение должно находиться в диапазоне от 0 до 7.

Значение по умолчанию

По умолчанию приоритету назначается значение 0.

Указания по использованию

Эта команда используется для назначения приоритета, по которому классу трафика по умолчанию выделяется дополнительная пропускная способность, когда она имеется.

Форма **set** этой команды используется для указания приоритета класса трафика по умолчанию.

Форма **delete** используется для восстановления приоритета по умолчанию класса трафика по умолчанию.

Форма **show** этой команды используется для отображения настройки приоритета класса трафика по умолчанию.

22.2.116 policy qos shaper <имя_политики> default queue-limit <ограничение>

Указание максимального размера очереди для класса трафика по умолчанию.

Синтаксис

```
set policy qos shaper <имя_политики> default queue-limit <ограничение>
delete policy qos shaper <имя_политики> default queue-limit
show policy qos shaper <имя_политики> default queue-limit
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      shaper имя_политики {
         default {
            queue-limit ограничение
         }
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

ограничение

Максимальный размер очереди в пакетах. Значение должно лежать в диапазоне 1-4294967295.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки максимального размера (в пакетах) очереди класса по умолчанию.

Форма **set** этой команды используется для указания ограничения длины очереди.

Форма **delete** этой команды используется для удаления ограничения длины очереди.

Форма **show** этой команды используется для отображения настройки ограничения длины очереди.

22.2.117 policy qos shaper <имя_политики> default queue-ref <имя_политики>

Указание дочерней политики QoS по умолчанию.

Синтаксис

```
set policy qos shaper <имя_политики> default queue-ref <имя_политики>
delete policy qos shaper <имя_политики> default queue-ref
show policy qos shaper <имя_политики> default queue-ref
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      shaper имя_политики {
         default {
            queue-ref имя_политики
         }
      }
   }
}
```

Параметры

shaper *имя_политики*

Обязательный. Имя политики управления загрузкой канала.

queue-ref *имя_политики*

Необязательный. Имя дочерней политики QoS.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная дочерняя политика будет применяться ко всему трафику, не соответствующему никакому другому определённому классу в рамках указанной политики.

Форма **set** этой команды используется для указания дочерней политики QoS.

Форма **delete** этой команды используется для удаления дочерней политики QoS.

Форма **show** этой команды используется для отображения настройки использования дочерней политики QoS.

22.2.118 policy qos shaper <имя_политики> default queue-type <тип>

Указание типа работы с очередью, используемого для класса трафика по умолчанию.

Синтаксис

```
set policy qos shaper <имя_политики> default queue-type <тип>
delete policy qos shaper <имя_политики> default queue-type
show policy qos shaper <имя_политики> default queue-type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   qos {
      shaper имя_политики {
         default {
            queue-type тип
         }
      }
   }
}
```

Параметры

имя_политики

Обязательный. Имя политики управления загрузкой канала.

тип

Используемый метод работы с очередями. Допустимые значения представлены в таблице ниже.

Таблица 208 – Допустимые типы очередей

Значение	Описание
fair-queue	Используется очередь SFQ.
drop-tail	Используется очередь FIFO.
priority	Приоритет в очереди устанавливается по значениям поля DSCP в байте ToS заголовка IP.
random-detect	Используется очередь RED.

Значение по умолчанию

По умолчанию используется тип fair-queue.

Указания по использованию

Эта команда используется для установки типа механизма работы с очередями, используемого в классе трафика по умолчанию.

Форма **set** этой команды используется для указания типа очереди.

Форма **delete** этой команды используется для восстановления типа очереди по умолчанию.

Форма **show** этой команды используется для отображения настройки типа очереди.

22.2.119 show incoming

Отображение входящих политик QoS.

Синтаксис

```
show incoming [<тип_интерфейса> [<интерфейс>]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

тип_интерфейса

Необязательный. Тип интерфейса.

интерфейс

Необязательный. Указание имени конкретного интерфейса.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения входящих политик QoS.

22.2.120 show queueing

Отображение текущих политик QoS.

Синтаксис

```
show queueing [<тип_интерфейса> [<интерфейс>]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

тип_интерфейса

Необязательный. Тип интерфейса.

интерфейс

Необязательный. Указание имени конкретного интерфейса.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения текущих политик QoS.

Примеры

В примере ниже приведен вывод всех политик QoS.

Пример 202 – "show queueing": отображение всех политик QoS

```
admin@edge:~$ show queueing
Interface  Policy                 Sent    Dropped  Overlimit
eth2       default               76687          0          0
eth3       shaper                    0          0          0
ethm       default                 776          0          0
lo         [noqueue]                 0          0          0
```

23 VRRP

23.1 Настройка VRRP

В этой главе рассматриваются следующие вопросы:

- Примеры настройки VRRP
- Обзор VRRP

23.1.1 Примеры настройки VRRP

В этой главе рассматриваются следующие вопросы:

- Настройка базовой конфигурации VRRP.
  - Пример настройки главного маршрутизатора
  - Пример настройки резервного маршрутизатора
- Настройка конфигурации VRRP с использованием синхронных групп.
  - Пример настройки главного маршрутизатора с использованием синхронных групп
  - Пример настройки резервного маршрутизатора с использованием синхронных групп
- Настройка конфигурации VRRP с использованием одного адреса
  - Пример настройки главного маршрутизатора в качестве владельца VIP-адреса
  - Пример настройки резервного маршрутизатора без адреса на интерфейсе
- Настройка конфигурации VRRP с использованием отдельного интерфейса для отправки объявлений.
  - Пример настройки главного маршрутизатора.
  - Пример настройки резервного маршрутизатора.

Настройка базовой конфигурации VRRP

В данной секции рассматриваются следующие вопросы:

- Пример настройки главного маршрутизатора.
- Пример настройки резервного маршрутизатора.

После завершения настройки система будет иметь конфигурацию, представленную на рисунке:

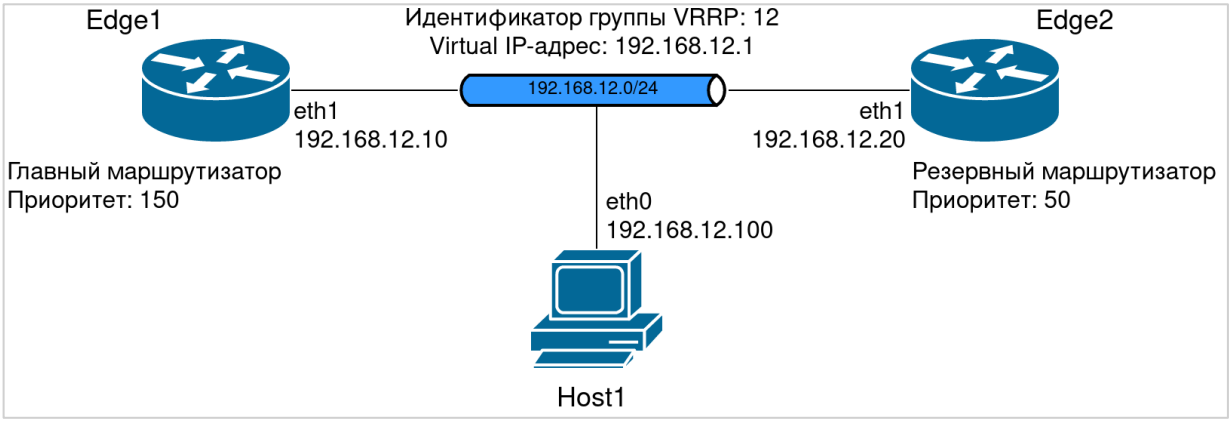


Рисунок 51 – Базовая конфигурация

Пример настройки главного маршрутизатора

В этом примере описывается настройка VRRP на интерфейсе Ethernet eth1 главного маршрутизатора (edge1) и его присоединение к виртуальному маршрутизатору с идентификатором 12.

- Интрефейсу eht1 назначается IP адрес 192.168.12.10/24;
- VIP-адрес: 192.168.12.1;
- Устанавливается значение приоритета равное 150;
- Включается режим приема пакетов устройством, не являющимся владельцем VIP-адреса (accept-mode);

- Вытеснение включено по умолчанию.

Пример 203 – Настройка главного маршрутизатора

Действие	**Команда**
Указание IP-адреса для интерфейса eth1 на маршрутизаторе edge1	`[edit]` `admin@edge1# set interfaces ethernet eth1 address 192.168.12.10/24`
Создание узла конфигурации VRRP для интерфейса eth1 на маршрутизаторе edge1. Это действие также включает VRRP на данном интерфейсе. Назначение VRID	`[edit]` `admin@edge1# set interfaces ethernet eth1 vrrp 12`
Указание VIP-адреса	`[edit]` `admin@edge1# set interfaces ethernet eth1 vrrp 12 virtual-address 192.168.12.1`
Включение режима приёма пакетов устройством, не являющимся владельцем VIP-адреса	`[edit]` `admin@edge1# set interfaces ethernet eth1 vrrp 12 accept-mode true`
Установка значения приоритета	`[edit]` `admin@edge1# set interfaces ethernet eth1 vrrp 12 priority 150`
Фиксация изменений	`[edit]` `admin@edge1# commit`

Отображение текущей конфигурации	`[edit]admin@edge1# show interfaces ethernet eth1 vrrp`
	`12 {`
	`accept-mode true`
	`priority 150`
	`virtual-address 192.168.12.1`
	`}`

Пример настройки резервного маршрутизатора

В этом примере описывается настройка VRRP на интерфейсе Ethernet eth1 резервного маршрутизатора (edge2) и его присоединение к виртуальному маршрутизатору 12.

- Интрефейсу eht1 назначается IP адрес 192.168.12.20/24;
- VIP-адрес остаётся таким же: 192.168.12.1;
- Устанавливается значение приоритета равное 50;
- Включается режим приема пакетов устройством, не являющимся владельцем VIP-адреса (accept-mode);
- Вытеснение включено по умолчанию.

Пример 204 – Настройка резервного маршрутизатора.

Действие	**Команда**
Указание IP-адреса для интерфейса eth1 на маршрутизаторе edge2	`[edit]` `admin@edge2# set interfaces ethernet eth1 address 192.168.12.20/24`
Создание узла конфигурации VRRP для интерфейса eth1 на маршрутизаторе edge2. Это действие также включает VRRP на данном интерфейсе. Назначение VRID	`[edit]` `admin@edge2# set interfaces ethernet eth1 vrrp 12`
Указание VIP-адреса	`[edit]` `admin@edge2# set interfaces ethernet eth1 vrrp 12 virtual-address 192.168.12.1`
Включение режима приёма пакетов устройством, не являющимся владельцем VIP-адреса	`[edit]` `admin@edge2# set interfaces ethernet eth1 vrrp 12 accept-mode true`
Установка значения приоритета	`[edit]` `admin@edge2# set interfaces ethernet eth1 vrrp 12 priority 50`

Фиксация изменений	`[edit]admin@edge2# commit`

Отображение текущей конфигурации	`[edit]`
	`admin@edge2# show interfaces ethernet eth1 vrrp 12`
	`{`
	`  accept-mode true`
	`  priority 50`
	`  virtual-address 192.168.12.1`
	`}`

Настройка конфигурации VRRP с использованием одного адреса

На практике может возникнуть необходимость сократить количество адресов, используемых VRRP. В данной секции рассматриваются следующие вопросы:

- Пример настройки главного маршрутизатора.
- Пример настройки резервного маршрутизатора.

Этот пример сделан на основе базовой конфигурации. Основным отличием является то, что вместо трех различных IP адресов: 192.168.12.10 – Edge1.eth1, 192.168.12.20 – Edge2.eth1, 192.168.12. 1 – VIP адрес, используется только один IP адрес 192.168.12.1. На устройстве Edge1 он настраивается на интерфейсе eth1, а также используется в качестве VIP адреса. Тем самым интерфейс eth1 на Edge1 является владельцем VIP адреса, и имеет наиболее возможный приоритет 255. На устройстве Edge2 на интерфейсе eth1 IP адрес не настраивается, но вместо этого настраивается параметр **hello-source address**, который использоваться когда Edge2 станет главным маршрутизатором для отправки VRRP объявлений с адресом источника равным VIP адресу.

К плюсам данной конфигурации можно отнести возможность экономии адресного пространства при подключении, например, к сети провайдера и необходимости резервирования только одного внешнего IP адреса.К минусам – невозможность доступа на резервный.

После завершения настройки система будет иметь конфигурацию, представленную на рисунке:

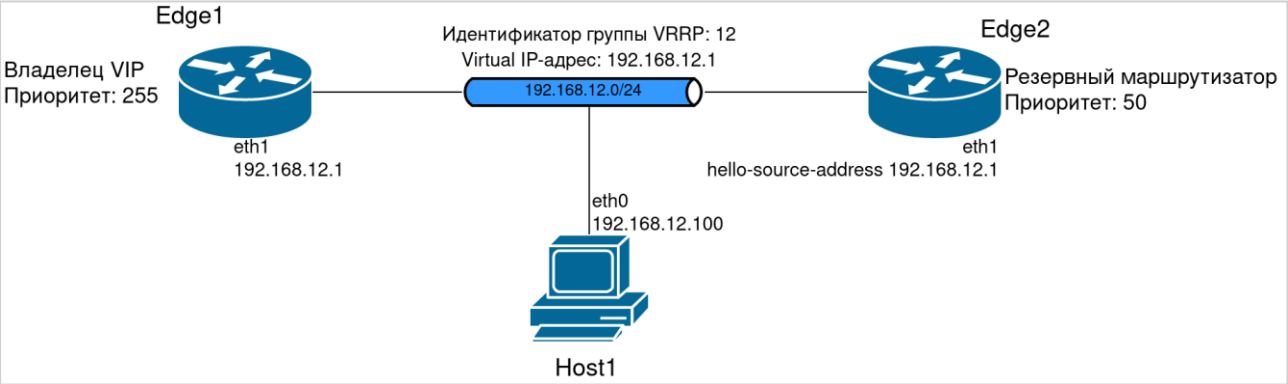


Рисунок 52 – Схема стенда

Пример настройки главного маршрутизатора в качестве владельца VIP-адреса

В данной секции приведён пример конфигурации интерфейса eth2 маршрутизатора Edge1 в качестве владельца VIP-адреса. Для этого существующие настройки интерфейса должны соответствовать следующим условиям:

- Интерфейс VRRP должен быть определён.
- IP-адрес интерфейса должен совпадать с VIP-адресом VRRP.
- Вытеснение должно быть включено – включено по уполчанию.
- Значение приоритета для интерфейса eth1 не должно быть задано.

Для назначения интерфейса eth1 владельцем VIP-адреса необходимо выполнить следующие действия:

Пример 205 – Настройка владельца VIP-адреса

Действие	**Команда**

Действие	Команда
Удаление IP-адреса для интерфейса eth1 на маршрутизаторе edge2.	[edit] admin@edge1# delete interfaces ethernet eth1 address
Удаление IP-адреса для интерфейса eth1 на маршрутизаторе edge2.	[edit] admin@edge1# delete interfaces ethernet eth1 vrrp 12 priority
Настройка адреса источника VRRP объявлений, в случае, когда устройство станет главным маршрутизатором.	[edit] admin@edge1# set interfaces ethernet eth1 address 192.168.12.1/24
Фиксация изменений	[edit] admin@edge1# commit

Отображение текущей конфигурации	[edit]
	admin@edge2# show interfaces ethernet eth1 address 192.168.12.1/24vrrp 12 {
	accept-mode true
	virtual-address 192.168.12.1
	}

Пример настройки резервного маршрутизатора без адреса на интерфейсе

В данной секции приведён пример конфигурации интерфейса eth1 маршрутизатора Edge2 без адреса на интерфейсе. Для этого существующие настройки интерфейса должны соответствовать следующим условиям:

- Интерфейс VRRP должен быть определён.
- Для интерфейса VRRP должен быть определен адрес VRRP объявлений. В качестве него будет задействован VIP-адрес.
- Вытеснение должно быть включено – включено по умолчанию.
- Дополнительно включим режим приема пакетов устройством, не являющимся владельцем VIP-адреса (accept-mode).
- Создание статического маршрута через интерфейс для подсети 192.168.12.0/24.

Для настройки интерфейса eth1 в качестве участника VRRP группы без адреса на интерфейсе необходимо выполнить следующие действия:

Пример 206 – Настройка интерфейса без адреса

Действие	Команда
Удаление IP-адреса для интерфейса eth1 на маршрутизаторе edge2.	[edit] admin@edge2# delete interfaces ethernet eth1 address
Настройка адреса источника VRRP объявлений, в случае, когда устройство станет главным маршрутизатором.	[edit] admin@edge2# set interfaces ethernet eth1 vrrp 12 hello-source-address 192.168.12.1
Фиксация изменений.	[edit] admin@edge1# commit

Отображение текущей конфигурации	[edit]
	admin@edge2# show interfaces ethernet eth1
	vrrp 12 {
	accept-mode true
	priority 50
	hello-source-address 192.168.12.1
	virtual-address 192.168.12.1
	}

После примерения данных необходимо еще создать отдельный статический маршрут для подсети, в которую входит VIP адрес. Это необходимо сделать потому что, сам VIP адрес задается с маской /32. Обычно при настройке IP адреса на определенном интерфейсе создается connected маршрут, ограниченный маской задаваемого IP адреса. В этом конкретном случае IP адрес на интерфейсе eth1 мы не задаем, и поэтому необходимо настроить вручную статический маршрут для подсети 192.168.12.0/24 через интерфейс eth1.

Действие	Команда
Создание статического маршрута для подсети 192.168.12.0/24 на интерфейс eth1.	[edit] admin@edge2# set protocols static interface-route 192.168.12.0/24 next-hop-interface eth1
Фиксация изменений.	[edit] admin@edge2# commit

Настройка конфигурации VRRP с использованием синхронных групп

В данной секции рассматриваются следующие вопросы:

- Пример настройки главного маршрутизатора.
- Пример настройки резервного маршрутизатора.

Этот пример сделан на основе базовой конфигурации. Настраивается VRRP на интерфейсах в сторону провайдера (eth2). После определения идентификатора виртуального маршрутизатора (VRID) и VIP-адреса на интерфейсах обоих маршрутизаторов, все задействованные интерфейсы объединяются в синхронную группу.

После завершения настройки система будет иметь конфигурацию, представленную на рисунке:

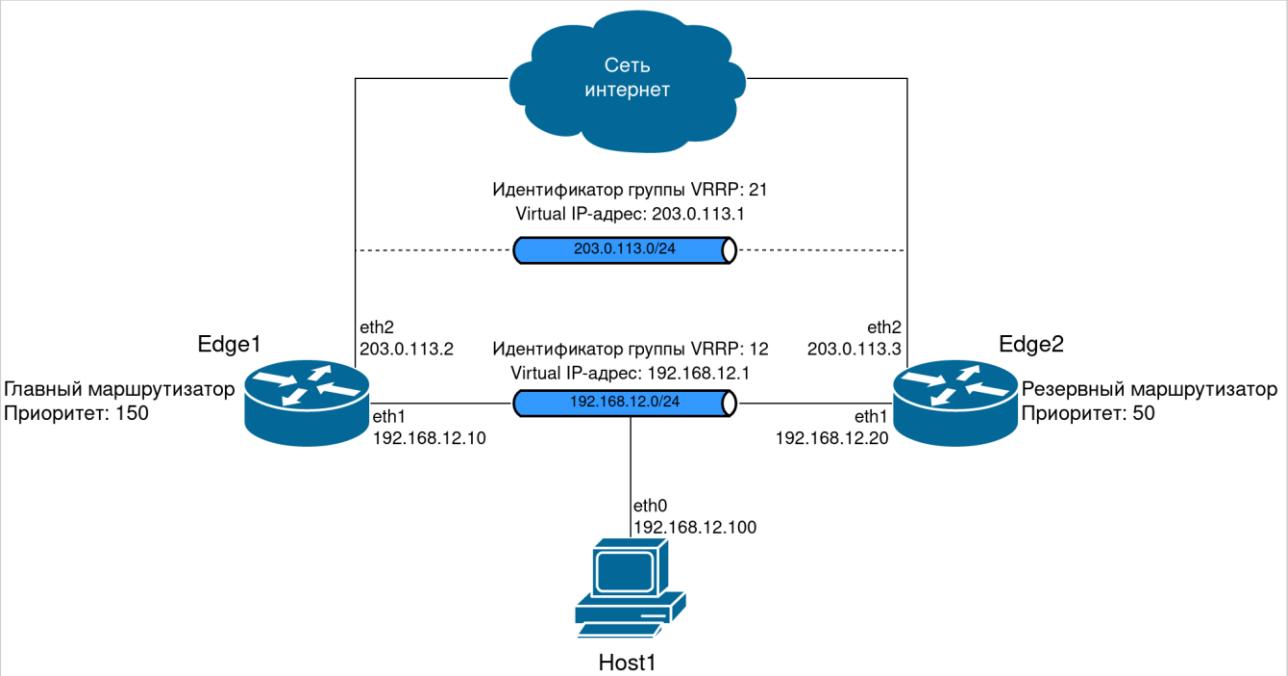


Рисунок 53 – Конфигурация VRRP с использованием синхронных групп

Пример настройки главного маршрутизатора с использованием синхронных групп

В этом примере описывается настройка VRRP на интерфейсе Ethernet eth1 главного маршрутизатора (edge1) и его присоединение к виртуальному маршрутизатору с идентификатором 21.

- VIP-адрес: 203.0.113.1. Вытеснение включено.
- Устанавливается значение приоритета равное 150.
- Интерфейсы eth1 и eth2 входят в группу синхронизации MAIN.
- Включается режим приема пакетов устройством, не являющимся владельцем VIP-адреса (accept-mode).
- Вытеснение включено по умолчанию.

Пример 207 – Настройка главного маршрутизатора с использованием синхронных групп

Действие	Команда
Добавление виртуального маршрутизатора 12 на интерфейсе eth1 к синхронной группе MAIN	[edit] admin@edge1# set interfaces ethernet eth1 vrrp 12 sync-group MAIN

Действие	Команда
Указание IP-адреса для интерфейса eth2 на маршрутизаторе edge1	[edit] admin@edge1# set interfaces ethernet eth2 address 203.0.113.2/29
Создание узла конфигурации VRRP для интерфейса eth2 маршрутизатора edge1. Это действе также включает VRRP на данном интерфейсе. Назначение VRID.	[edit] admin@edge1# set interfaces ethernet eth2 vrrp 21
Указание VIP-адреса.	[edit] admin@edge1# set interfaces ethernet eth2 vrrp 21 virtual-address 203.0.113.1
Включение режима приёма пакетов устройством, не являющимся владельцем VIP-адреса	[edit] admin@edge1# set interfaces ethernet eth2 vrrp 21 accept-mode true
Установка значения приоритета.	[edit] admin@edge1# set interfaces ethernet eth2 vrrp 21 priority 150
Добавление виртуального маршрутизатора 21 на интерфейсе eth2 к синхронной группе MAIN	[edit] admin@edge1# set interfaces ethernet eth2 vrrp 21 sync-group MAIN
Фиксация изменений	[edit] admin@edge1# commit

Отображение текущей конфигурации	[edit]
	admin@edge1# show interfaces ethernet eth1 vrrp 12 {
	priority 150
	strict-mode
	sync-group MAIN
	virtual-address 192.168.12.1 }
	[edit]
	admin@edge1# show interfaces ethernet eth2 vrrp
	21 {
	priority 150
	strict-mode
	sync-group MAIN
	virtual-address 203.0.113.1
	}

Пример настройки резервного маршрутизатора с использованием синхронных групп

В этом примере описывается настройка VRRP на интерфейсе Ethernet eth1 резервного маршрутизатора (edge2) и его присоединение к виртуальному маршрутизатору.

- VIP-адрес виртуального маршрутизатора 21 остаётся таким же: 203.0.113.1.
- Включается режим приема пакетов устройством, не являющимся владельцем VIP-адреса (accept-mode).
- Устанавливается значение приоритета равное 50.
- Интерфейсы eth1 и eth2 входят в группу синхронизации MAIN.
- Вытеснение включено по умолчанию.

Пример 208 – Настройка резервного маршрутизатора с использованием синхронных групп

Действие	Команда
Добавление виртуального маршрутизатора 12 на интерфейсе eth1 к синхронной группе MAIN	[edit] admin@edge2# set interfaces ethernet eth1 vrrp 12 sync-group MAIN
Указание IP-адреса для интерфейса eth2 на маршрутизаторе edge2	[edit] admin@edge2# set interfaces ethernet eth2 address 203.0.113.3/29
Создание узла конфигурации VRRP для интерфейса	[edit]

Действие	Команда
eth2 маршрутизатора edge2. Это действе также включает VRRP на данном интерфейсе. Назначение VRID.	admin@edge2# set interfaces ethernet eth2 vrrp 21
Указание VIP-адреса.	[edit] admin@edge2# set interfaces ethernet eth2 vrrp 21 virtual-address 203.0.113.1
Включение режима приёма пакетов устройством, не являющимся владельцем VIP-адреса	[edit] admin@edge2# set interfaces ethernet eth2 vrrp 21 accept-mode true
Установка значения приоритета.	[edit] admin@edge2# set interfaces ethernet eth2 vrrp 21 priority 50
Добавление виртуального маршрутизатора 201 на интерфейсе eth2 к синхронной группе MAIN	[edit] admin@edge2# set interfaces ethernet eth2 vrrp 21 sync-group MAIN
Фиксация изменений	[edit] admin@edge2# commit

Отображение текущей конфигурации	[edit]
	admin@edge2# show interfaces ethernet eth1 vrrp
	  12 {
	  priority 50
	  strict-mode
	  sync-group MAIN
	  virtual-address 192.168.12.1
	  }
	[edit]
	admin@edge2# show interfaces ethernet eth2 vrrp
	  21 {
	  priority 50
	  strict-mode
	  sync-group MAIN
	  virtual-address 203.0.113.1
	  }

Настройка конфигурации VRRP с использованием отдельного интерфейса для отправки объявлений.

В данной секции рассматриваются следующие вопросы:

- Пример настройки главного маршрутизатора.
- Пример настройки резервного маршрутизатора.

Этот пример сделан на основе предыдущего. Во всех предыдущих примерах VRRP объявления отправлялись на multicast адрес 224.0.0.18, который определен стандартами RFC 3768 (для VRRP версии 2) и RFC 5798 (для VRRP версии 3). Эти объявления отправлялись с интерфейсов виртуальных маршрутизаторов (eth1 и eth2).

В этом примере добавляется дополнительный интерфейс (eth3), через который будут отправляться объявления VRRP виртуальных маршрутизаторов 12 и 21. Этому интерфейсу назначаются unicast адреса 10.10.10.1 для устройства edge1 и 10.10.10.2 для edge2. В начальном состоянии, когда оба устройства работают корректно – edge1 является главным маршрутизатором, согласно наибольшего приоритета. Он отправляет VRRP объявления с адресом назначения 10.10.10.2 и адресом источника 10.10.10.1 через интерфейс eth3.

После завершения настройки система будет иметь конфигурацию, представленную на рисунке:

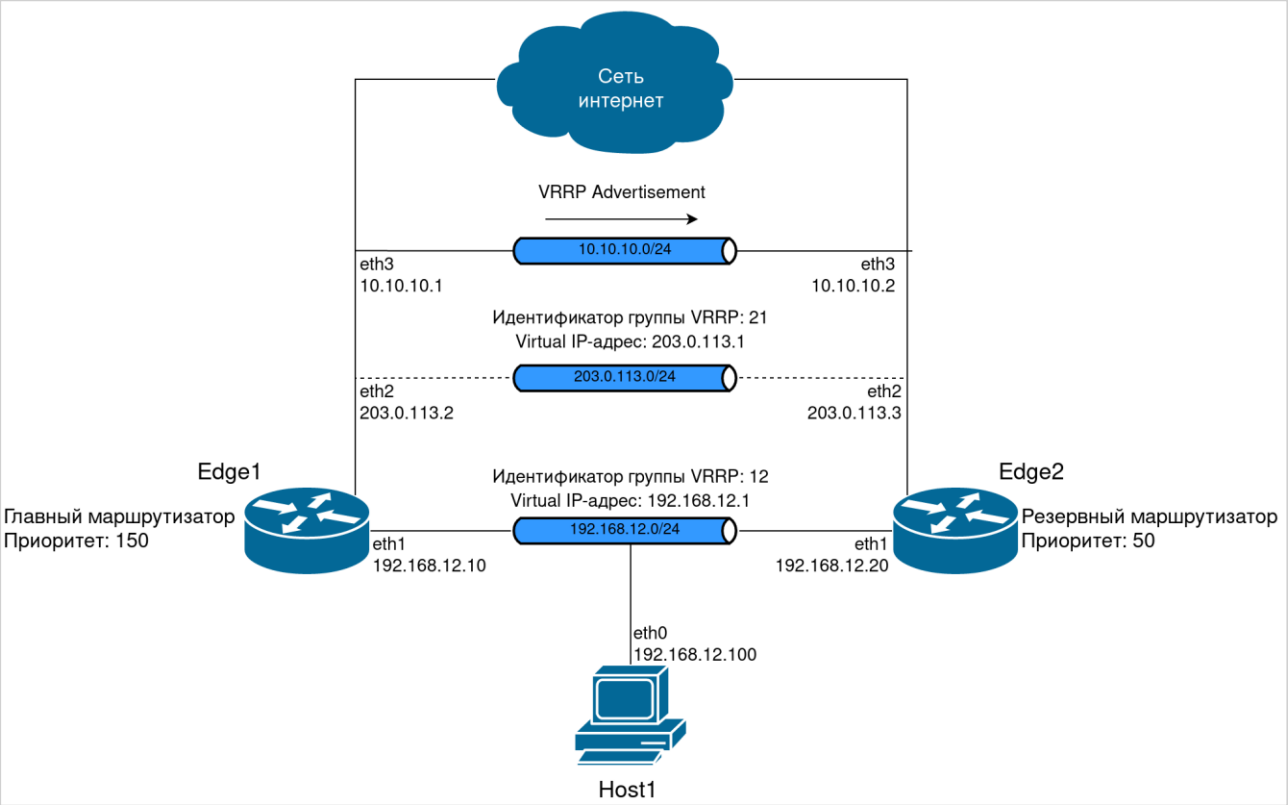


Рисунок 54 – Конфигурация VRRP с использованием отдельного интерфейса для отправки сообщения

Пример настройки главного маршрутизатора

Пример 209 – Настройка главного маршрутизатора, с использованием отдельного интерфейса для отправки VRRP объявлений

Действие	**Команда**
Добавления IP адреса на интерфейс eht3, используемый для отправки VRRP объявлений.	`[edit]admin@edge1# set interfaces ethernet eth3 address 10.10.10.1/24`
Указание отдельного интерфейса для отправки VRRP объявлений для виртуального маршрутизатора 21.	`[edit]admin@edge1# set interfaces ethernet eth1 vrrp 21 interface 'eth3'`
Использование в качестве адреса отправителя, настроенный ранее IP адрес на интерфейсе eth3.	`[edit] admin@edge1# set interfaces ethernet eth1 vrrp 21 hello-source-address '10.10.10.1'`
В качестве адреса назначения используется unicast IP адрес, который будет настроен на интерфейсе eth3 устройства edge2.	`[edit] admin@edge1# set interfaces ethernet eth1 vrrp 21 unicast-peers '10.10.10.2'`
Указание отдельного интерфейса для отправки VRRP объявлений для виртуального маршрутизатора 12.	`[edit]admin@edge1# set interfaces ethernet eth2 vrrp 12 interface 'eth3'`
Использование в качестве адреса отправителя, настроенный ранее IP адрес на интерфейсе eth3.	`[edit]admin@edge1# set interfaces ethernet eth2 vrrp 12 hello-source-address '10.10.10.1'`
В качестве адреса назначения используется unicast IP адрес, который будет настроен на интерфейсе eth3 устройства edge2.	`[edit]admin@edge1# set interfaces ethernet eth2 vrrp 12 unicast-peers '10.10.10.2'`
Применение изменений.	`[edit]admin@edge1# commit`
Отображение текущей конфигурации.	`[edit]admin@edge1# admin@edge1# show interfaces ethernet eth1 vrrp 21 { accept-mode true`

	hello-source-address 10.10.10.1
	interface eth3
	preempt true
	priority 150
	unicast-peers 10.10.10.2
	virtual-address 192.168.12.1
	}
	[edit]admin@edge1# admin@edge1# show interfaces ethernet eth2 vrrp
	12 {
	accept-mode true
	hello-source-address 10.10.10.1
	interface eth3
	preempt true
	priority 150
	sync-group MAIN
	unicast-peers 10.10.10.2
	virtual-address 203.0.113.1
	}
	[edit]
	admin@edge1# show interfaces ethernet eth3
	address 10.10.10.1/24
	[edit]
	admin@edge1#

Пример настройки резервного маршрутизатора

Пример 210 – Настройка резервного маршрутизатора, с использованием отдельного интерфейса для отправки VRRP объявлений

Действие	Команда
Добавления IP адреса на интерфейс eht3, используемый для получения VRRP объявлений. Либо отправки, если устройство является главным маршрутизатором.	[edit]admin@edge2# set interfaces ethernet eth3 address 10.10.10.2/24
Указание отдельного интерфейса для отправки VRRP объявлений для виртуального маршрутизатора 21.	[edit]admin@edge2# set interfaces ethernet eth1 vrrp 21 interface 'eth3'
Использование в качестве адреса отправителя, настроенный ранее IP адрес на интерфейсе eth3.	[edit]admin@edge2# set interfaces ethernet eth1 vrrp 21 hello-source-address '10.10.10.1'
В качестве адреса назначения используется unicast IP адрес, который будет настроен на интерфейсе eth3 устройства edge2.	[edit]admin@edge2# set interfaces ethernet eth1 vrrp 21 unicast-peers '10.10.10.2'
Указание отдельного интерфейса для отправки VRRP объявлений для виртуального маршрутизатора 12.	[edit]admin@edge2# set interfaces ethernet eth2 vrrp 12 interface 'eth3'
Использование в качестве адреса отправителя, настроенный ранее IP адрес на интерфейсе eth3.	[edit]admin@edge2# set interfaces ethernet eth2 vrrp 12 hello-source-address '10.10.10.1'
В качестве адреса назначения используется unicast IP адрес, который будет настроен на интерфейсе eth3 устройства edge2.	[edit]admin@edge2# set interfaces ethernet eth2 vrrp 12 unicast-peers '10.10.10.2'
Применение изменений.	[edit]admin@edge2# commit
Отображение текущей конфигурации.	admin@edge1# show interfaces ethernet eth1 vrrp 21 { accept-mode true hello-source-address 10.10.10.2 interface eth3 preempt true

```
      priority                        150
      unicast-peers          10.10.10.1
      virtual-address      192.168.12.1
  }
[edit]
admin@edge1# show interfaces ethernet
eth2              vrrp
  12                                   {
      accept-mode                    true
      hello-source-address  10.10.10.2
      interface                      eth3
      preempt                        true
      priority                        150
      sync-group                     MAIN
      unicast-peers          10.10.10.1
      virtual-address       203.0.113.1
  }
[edit]
admin@edge1# show interfaces ethernet
eth3
  address                 10.10.10.2/24
[edit]
admin@edge1#
```

23.1.2 Обзор VRRP

В данном разделе представлены следующие темы:

- Протокол VRRP
- Идентификатор виртуального маршрутизатора (VRID)
- VIP-адрес
- Владелец VIP-адреса
- Виртуальный MAC-адрес
- Интерфейс VRRP
- Объявления VRRP
- Выбор главного маршрутизатора
- Вытеснение
- Аутентификация VRRP
- Синхронные группы VRRP
- Фильтрация по состоянию
- Поддержка SNMP для VRRP

Протокол VRRP

Virtual Router Redundancy Protocol (VRRP) — сетевой протокол, позволяющий объединять группу маршрутизаторов в один виртуальный маршрутизатор. VRRP предназначен для обеспечения отказоустойчивости маршрутизатора, выполняющего роль шлюза по умолчанию.

В Numa Edge реализована поддержка VRRP по стандарту RFC 3768 для физических интерфейсов Ethernet, виртуальных интерфейсов на интерфейсах Ethernet, интерфейсов агрегированных каналов Ethernet и виртуальных интерфейсов на интерфейсах агрегированных каналов Ethernet..

ПРИМЕЧАНИЕ В силу ограничений текущей реализации протоколов DHCP и VRRP, их использование на одном и том же интерфейсе невозможно. При использовании протокола VRRP IP-адрес на интерфейсе может быть задан только статически.

Идентификатор виртуального маршрутизатора (VRID)

При использовании VRRP, интерфейсы физических маршрутизаторов формируют «виртуальный маршрутизатор». Виртуальный маршрутизатор — это абстрактный объект, управляемый процессом VRRP и определяемый посредством его идентификатора и VIP-адреса. Узлы в сети настраиваются таким образом,

чтобы направлять пакеты на VIP-адрес виртуального маршрутизатора, вместо IP-адресов физических интерфейсов.

Виртуальный маршрутизатор может состоять из кластера физических и/или виртуальных интерфейсов, обеспечивающих резервирование для первичного (primary) интерфейса (мастер-интерфейса). Как правило, интерфейсы, входящие в виртуальный маршрутизатор, находятся на разных маршрутизаторах.

Резервированием управляет процесс VRRP, выполняемый в системе каждого маршрутизатора, состоящего в виртуальном маршрутизаторе.

Каждый виртуальный маршрутизатор имеет уникальный цифровой идентификатор (Virtual router ID — VRID) и виртуальный IP-адрес (Virtual IP — VIP). Каждому виртуальному маршрутизатору может быть назначено до 20 VIP-адресов. Для обеспечения резервирования интерфейсам в составе виртуального маршрутизатора должен быть назначен одинаковый идентификатор и VIP-адрес. IP-адреса интерфейсов и VIP-адрес группы не обязательно должны находится в одной подсети. Допускается использование интерфейсов, не имеющих IP-адреса (unnumbered).

Один интерфейс может входить в состав нескольких виртуальных маршрутизаторов.

VIP-адрес

Устройствам, состоящим в виртуальном маршрутизаторе, присваивается единый VIP-адрес. Таким образом обеспечиваются альтернативные пути маршрутизации для устройств, подключенных к сети, без необходимости изменения их настроек. Кроме того, таким образом обеспечивается резервирование существующих маршрутов, благодаря чему отдельный маршрутизатор не может стать компонентом, отказ которого приводит к отказу всей сети (Single Point of Failure — SPOF).

Виртуальный маршрутизатор использует свой идентификатор и MAC-префикс для создания виртуального MAC-адреса. ARP-запросы к VIP передаются на виртуальный MAC-адрес, который в свою очередь, присваивается физическому маршрутизатору, задействованному в этот момент в качестве главного маршрутизатора. При отказе главного маршрутизатора виртуальный MAC-адрес и VIP присваиваются одному из резервных устройств, после того, как резервный маршрутизатор становится главным. Таким образом обеспечивается непрерывный доступ узлов к шлюзу даже в случае отказа одного из устройств в рамках виртуального маршрутизатора.

Главный маршрутизатор перенаправляет пакеты, предназначенные локальным устройствам, отвечает на ARP-запросы, сообщения ping через протокол ICMP и IP-датаграммы, направляемые на VIP-адрес. При этом резервные маршрутизаторы бездействуют, даже в случае отсутствия сбоев. На ARP-запросы и сообщения ping, а также IP-датаграммы, посылаемые на реальные IP-адреса собственных интерфейсов, резервный маршрутизатор отвечает обычным образом.

Владелец VIP-адреса

Маршрутизатор является владельцем VIP-адреса в том случае, если основным IP-адресом интерфейса с VRRP является VIP-адрес. При назначении VIP-адреса интерфейсу, данный интерфейс получает преимущественное право на его использование. Настройки интерфейса, являющегося владельцем VIP-адреса должны соответствовать следующим условиям:

- Владелец VIP-адреса не должен иметь другого заданного IP-адреса.
- Настройки VRRP должны быть определены для владельца VIP-адреса.
- Вытеснение (preemption) должно быть включено (enable).
- Источник получения «hello» пакетов должен соответствовать установленному по умолчанию.

Значением приоритета для владельца VIP-адреса всегда будет 255. Это значение зарезервировано и его нельзя настроить вручную. Доступный диапазон настройки приоритета 1-254. Таки образом, маршрутизатор владелец VIP не может быть резервным маршрутизатором.

ПРИМЕЧАНИЕ В случае использования нескольких VIP-адресов возможна ситуация, когда IP-адреса сразу нескольких устройств совпадут с VIP-адресами в рамках одного виртуального маршрутизатора и станут владельцами VIP-адресов — главными маршрутизаторами, такая ситуация может привести к проблемам функционирования сети. Данный случай настройки виртуального маршрутизатора не противоречит спецификации стандарта RFC 3768. Рекомендуется учитывать это при конфигурировании VIP-адресов в рамках одного виртуального маршрутизатора, чтобы исключить одновременное появление нескольких владельцев VIP-адресов.

Виртуальный MAC-адрес

Согласно спецификации RFC 3768, каждому виртуальному маршрутизатору VRRP должен быть присвоен определённый 48-битный MAC-адрес. Виртуальный MAC-адрес создаётся на основе MAC-префиксов (описанных в спецификации протокола VRRP) и идентификатора виртуального маршрутизатора. Виртуальный MAC-адрес выглядит как 0000:5E00:01xx, где xx — идентификатор виртуального маршрутизатора.

Главный маршрутизатор использует MAC-адрес виртуального маршрутизатора в качестве источника для отправляемых VRPP-пакетов. При получении статуса главного маршрутизатора, резервное устройство также начинает использовать MAC-адрес виртуального маршрутизатора.

Использование предопределённого MAC-адреса виртуального маршрутизатора позволяет не менять настройки ARP при сбое главного маршрутизатора.

В системе Numa Edge присутствует поддержка альтернативного режима присвоения MAC-адреса. В данном режиме VIP-адрес будет присваиваться MAC-адресу главного маршрутизатора. В случае сбоя, VIP-адрес присваивается MAC-адресу резервного маршрутизатора, который в свою очередь извещает об изменении MAC-адреса посредством самообращённых запросов ARP.

По умолчанию, система Numa Edge использует альтернативный режим присвоения MAC-адреса. Настройка режима присвоения MAC-адреса осуществляется параметром **interfaces <интерфейс> vrrp <идентификатор> strict-mode**

ПРИМЕЧАНИЕ. Устройства, состоящие в одном виртуальном маршрутизаторе должны использовать одинаковые режимы присвоения MAC-адреса.

Интерфейс VRRP

Интерфейс VRRP функционирует в режиме прохождения (pass-through). Данный режим позволяет получать пакеты, направляемые на виртуальный MAC-адрес виртуального маршрутизатора на интерфейс главного маршрутизатора. Интерфейс VRRP используется для передачи пакетов протокола VRRP. Пакеты протокола VRRP предназначены для передачи информации о состоянии и приоритете главного маршрутизатора остальным устройствам, состоящим в виртуальном маршрутизаторе.

Имя интерфейса VRRP назначается автоматически на основе идентификатора используемого интерфейса главного маршрутизатора и идентификатора виртуального маршрутизатора.

Таблица 209 — Формат имени интерфейса VRRP

Формат	Тип интерфейса	Идентификатор интерфейса и идентификатор виртуального маршрутизатора (VRID)	Имя интерфейса VRRP
eth*n*v*V*	Физический интерфейс Ethernet	eth1 и VRID 21	eth1v21
bond*n*v*V*	Интерфейс агрегированных каналов Ethernet	bond1 и VRID 12	bond1v12
eth*n.D*v*V*	Виртуальный интерфейс на интерфейсе Ethernet	eth1, VLAN ID 10, VRID 21	eth1.10v21
Bond*n.D*v*V*	Виртуальный интерфейс на интерфейсе агрегированных каналов Ethernet	bond1, VLAN ID 10, VRID 12	Bond1.10v12

Объявления VRRP

Главный маршрутизатор использует объявления VRRP для передачи информации о своём текущем состоянии резервным маршрутизаторам. Объявления VRRP состоят из пакетов «heartbeat», которые содержат информацию о состоянии главного маршрутизатора и его приоритет. В каждом виртуальном маршрутизаторе только главный маршрутизатор отправляет периодические объявления VRRP на зарезервированный адрес 224.0.0.18. На канальном уровне в качестве MAC-адреса отправителя объявлений VRRP используется виртуальный MAC-адрес. Если резервные устройства не получают объявления VRRP в течении заданного периода (dead interval), то главный маршрутизатор считается неработоспособным, после чего статус главного маршрутизатора присваивается одному из резервных маршрутизаторов согласно выставленному значению приоритета.

Выбор главного маршрутизатора

Выбор главного устройства в рамках виртуального маршрутизатора происходит автоматически на основании выставленного значения приоритета. Если у двух устройств в составе виртуального маршрутизатора значение приоритета будет равным, то главным маршрутизатором назначается маршрутизатор с большим IP-адресом.

При отказе мастер-интерфейса, дублирующий интерфейс с наибольшим значением приоритета назначается мастер-интерфейсом и ему присваивается VIP-адрес виртуального маршрутизатора.

Рекомендуется устанавливать значение приоритета мастер-интерфейса равным наибольшему значению приоритета дублирующего интерфейса плюс 50. Значение приоритета дублирующего интерфейса можно оставить равным значению по умолчанию, однако при наличии двух и более дублирующих интерфейсов, следует задать им разные значения приоритета.

Возможные состояния виртуального маршрутизатора на устройствах

Таблица 210 — Формат имени интерфейса VRRP

Состояние	Описание
MASTER	Главный маршрутизатор – это устройство, имеющее наибольший приоритет в рамках одного виртуального маршрутизатора. Отправляет на резервные маршрутизаторы объявления, содержащие в том числе, значение приоритета.
BACKUP	Резервный маршрутизатор – это устройство, которое имеет меньший приоритет чем главный маршрутизатор. При получении объявлений сравнивает приоритет в полученном обявлении со своим значением. Если было получено объявление с меньшим приоритетом или объявления не были получены в течении установленного интервала – резервный маршрутизатор становится главным маршрутизатором.
FAUIL	Состояние ошибки – в большинстве случаев, связано с выходом из строя/отключением интерфейса, связанного с виртуальным маршрутизатором.

Вытеснение

При включенном параметре вытеснения (preempt) резервный маршрутизатор с большим приоритетом чем у текущего главного маршрутизатора будет замещать главный маршрутизатор, посылая свои собственные объявления VRRP. После того, как главный маршрутизатор обнаружит, что у дублирующего устройства задано более высокое значение приоритета, он прекращает посылать объявления VRRP. Таким образом дублирующий маршрутизатор с более высоким значением приоритета назначается главным маршрутизатором.

Вытеснение полезно в случае нахождения в одном виртуальном маршрутизаторе высокопроизводительного главного маршрутизатора и низкопроизводительного резервного маршрутизатора. Например, при сбое главного маршрутизатора, малопроизводительный резервный маршрутизатор назначается главным маршрутизатором до момента устранения сбоя. После устранения сбоя высокопроизводительный маршрутизатор с большим приоритетом будет автоматически назначен главным маршрутизатором.

В системе Numa Edge вытеснение включено по умолчанию.

Аутентификация VRRP

При настройке аутентификации VRRP помимо пароля необходимо указать тип аутентификации. Если пароль установлен, а тип аутентификации не определён, то система генерирует ошибку при фиксации изменений конфигурации (commit). По той же причине нельзя удалить пароль без удаления типа аутентификации.

При удалении типа аутентификации VRRP и пароля, аутентификация VRRP автоматически отключается.

Синхронные группы VRRP

При конфигурации на одном устройстве нескольких виртуальных маршрутизаторов, для каждого из них состояние отслеживается отдельно. Синхронные группы VRRP позволяют объединить несколько таких виртуальных маршрутизаторов в общую группу. В этом случае, при изменении состояния одного из виртуальных маршрутизаторов – данное состояние принимают все остальные маршрутизаторы, объединенные в синхронную группу.

ПРИМЕЧАНИЕ: Рекомендуется на всех интерфейсах, объединенных в синхронную группу для каждого устройства, задавать одинаковые значения приоритета.

Фильтрация по состоянию

Согласно спецификации VRRP, если процесс VRRP находится в состоянии BACKUP, то все пакеты, направленные на виртуальный MAC-адрес виртуального маршрутизатора должны игнорироваться (drop).

Поддержка SNMP для VRRP

Numa Edge поддерживает удаленный мониторинг VRRP через протокол SNMP. Система Numa Edge поддерживает объекты стандартов RFC 2787, RFC 6527, а также базу управляющей информации KEEPALIVED-MIB.

Клиент SNMP делает запрос через системную службу *snmpd*. Запрос перенаправляется системной службе *keepalived*, которая в свою очередь возвращает ответ на запрос согласно описанию KEEPALIVED-MIB. Таким образом, клиенту SNMP становится доступна специфическая дополнительная информация о состоянии VRRP, например, информация о состоянии главного маршрутизатора, синхронной группы и так далее.

OIDs:

- KEEPALIVED-MIB: iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) debian(9586) project(100) keepalived(5);
- RFC 2787: iso(1) identified-organization(3) dod(6) internet(1) mgmt(2) mib-2(1) vrrpMIB(68);
- RFC 6527: iso(1) identified-organization(3) dod(6) internet(1) mgmt(2) mib-2(1) vrrpv3MIB(207).

23.2 Команды VRRP

Режим настройки	
interfaces <интерфейс> vrrp <идентификатор>	Назначение идентификатора виртуального маршрутизатора для заданного интерфейса.
interfaces <интерфейс> vrrp <идентификатор> accept-mode <режим>	Установка режима приема пакетов устройством, не являющимся владельцем адреса.
interfaces <интерфейс> vrrp <идентификатор> advertise-interval <интервал>	Установка интервала отправки объявлений VRRP.
interfaces <интерфейс> vrrp <идентификатор> authentication password <пароль>	Установка пароля для виртуального маршрутизатора
interfaces <интерфейс> vrrp <идентификатор> authentication type <тип>	Установка типа аутентификации для виртуального маршрутизатора.
interfaces <интерфейс> vrrp <идентификатор> description <описание>	Указание текстового описания для виртуального маршрутизатора.
interfaces <интерфейс> vrrp <идентификатор> disable	Отключение виртуального маршрутизатора с сохранением существующей конфигурации.
interfaces <интерфейс> vrrp <идентификатор> hello-source-address <ipv4-адрес>	Указание источника пакетов анонса (advertisement messages) VRRP.
interfaces <интерфейс> vrrp <идентификатор> preempt <режим>	Включение или отключение режима вытеснения.
interfaces <интерфейс> vrrp <идентификатор> preempt-delay <задержка>	Указание задержки осуществления вытеснения.
interfaces <интерфейс> vrrp <идентификатор> priority <приоритет>	Установка значения приоритета для маршрутизатора рамках виртуального маршрутизатора.
interfaces <интерфейс> vrrp <идентификатор> strict-mode	Включение совместимости со стандартом RFC, указанным в узле version.
interfaces <интерфейс> vrrp <идентификатор> sync-group <имя_группы>	Добавление интерфейса в группу синхронизации.
interfaces <интерфейс> vrrp <идентификатор> version <версия_протокола>	Указание используемой версии протокола VRRP.

interfaces <интерфейс> vrrp <идентификатор> virtual-address <ipv4-адрес>	Указание VIP-адреса виртуального маршрутизатора.
interfaces <интерфейс> vrrp <идентификатор> interface <интерфейс>	Интерфейс для отправки и приема VRRP сообщений
interfaces <интерфейс> vrrp <идентификатор> unicast-peers <ipv4-адрес>	IP адреса назначения вместо группы многоадресной рассылки.
Эксплуатационный режим	
service vrrp restart	Перезапуск процесса VRRP.
service vrrp show	Отображение информации о настроенных интерфейсах VRRP.
show interfaces vrrp	Отображение информации о настроенных интерфейсах VRRP
show interfaces vrrp <идентификатор_vrrp_интерфейса> capture	Отображение трафика на интерфейсе VRRP

23.2.1 interfaces <интерфейс> vrrp <идентификатор>

Назначение группы VRRP для заданного интерфейса.

Синтаксис

```
set interfaces <интерфейс> vrrp <идентификатор>
delete interfaces <интерфейс> vrrp <идентификатор>
show interfaces <интерфейс> vrrp <идентификатор>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
   vrrp идентификатор {
   }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже:

Таблица 211 – Типы поддерживаемых интерфейсов, синтаксис и параметры команды

Тип интерфейса	Синтаксис	Параметры
Интерфейс агрегированных каналов Ethernet (bonding)	bonding *bondx*	*bondx* – идентификатор интерфейса агрегированных каналов Ethernet. Значение лежит в диапазоне **bond0-bond99**
Виртуальный интерфейс на интерфейсе агрегированных каналов Ethernet (bonding vif)	bonding *bondx* vif *vlan-id*	*bondx* – идентификатор интерфейса агрегированных каналов Ethernet. Значение лежит в диапазоне **bond0-bond99** *vlan-id* – идентификатор VLAN виртуального интерфейса. Значение лежит в диапазоне от 0 до 4094.
Ethernet	ethernet *ethx*	*ethx* – идентификатор интерфейса Ethernet. Значение лежит в диапазоне **eth0-eth999**, в зависимости от количества физических интерфейсов, доступных в системе.
Виртуальный интерфейс на интерфейсе Ethernet (Ethernet Vif)	ethernet *ethx* vif *vlan-id*	*ethx* – идентификатор интерфейса Ethernet. Значение лежит в диапазоне **eth0-eth999**, в зависимости от количества физических интерфейсов, доступных в

Тип интерфейса	Синтаксис	Параметры
		системе. vlan-id – идентификатор VLAN виртуального интерфейса. Значение лежит в диапазоне от 0 до 4094.

идентификатор

Числовой идентификатор виртуального маршрутизатора. Значение в диапазоне от 1 до 255.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет назначить идентификатор виртуального маршрутизатора для заданного интерфейса. Один интерфейс может состоять в нескольких виртуальных маршрутизаторах.

Форма **set** этой команды используется для присвоения данному интерфейсу идентификатора виртуального маршрутизатора (VRID).

Форма **delete** этой команды используется для удаления с данного интерфейса идентификатора виртуального маршрутизатора (VRID).

Форма **show** этой команды используется для просмотра настроек виртуального маршрутизатора для заданного интерфейса.

23.2.2 interfaces <интерфейс> vrrp <идентификатор> interface <интерфейс>

Интерфейс для отправки и приема VRRP сообщений.

Синтаксис

```
set interfaces <интерфейс> vrrp <идентификатор> interface <интерфейс>
delete interfaces <интерфейс> vrrp <идентификатор> interface
show interfaces <интерфейс> vrrp <идентификатор> interface
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
   vrrp идентификатор {
      interface интерфейс
   }
}
```

Параметры

Интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице в описании команды **interfaces <интерфейс> vrrp <идентификатор>**.

идентификатор

Числовой идентификатор виртуального маршрутизатора. Значение в диапазоне от 1 до 255.

интерфейс

Тип интерфейса. Позволяет использовать отдельный интерфейс для приема и отправки VRRP сообщений.

Значение по умолчанию

Отсутсвует.

Указания по использованию

Эта команда используется, если необходимо настроить отправку и получение VRRP объявлений на интерфейсе, отличном от интерфейса виртуального марштутизатора.

Форма **set** этой команды используется для указания отдельного интерфейса, для отправки и приема VRRP объявлений.

Форма **delete** этой команды используется для удаления отдельного интерфейса, для отправки и приема VRRP объявлений.

Форма **show** используется для просмотра текущей настройки интерфейса, для отправки и приема VRRP объявлений.

23.2.3 interfaces <интерфейс> vrrp <идентификатор> preempt <режим>

Включение или отключение вытеснения.

Синтаксис

```
set interfaces <интерфейс> vrrp <идентификатор> preempt <режим>
delete interfaces <интерфейс> vrrp <идентификатор> preempt
show interfaces <интерфейс> vrrp <идентификатор> preempt
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
   vrrp идентификатор {
      preempt режим
   }
}
```

Параметры

Интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице в описании команды **interfaces <интерфейс> vrrp <идентификатор>**.

идентификатор

Числовой идентификатор виртуального маршрутизатора. Значение в диапазоне от 1 до 255.

режим

Используемый режим вытеснения. Допустимые значения представлены в таблице ниже:

true: Вытеснение включено;

false: Вытеснение отключено.

Значение по умолчанию

По умолчанию вытеснение включено.

Указания по использованию

Эта команда позволяет включить или отключить режим вытеснения в указанном виртуальном маршрутизаторе. Если режим вытеснения включен, резервный маршрутизатор с высоким приоритетом вытесняет главный маршрутизатор с более низким значением приоритета. Таким образом, в рамках виртуального маршрутизатора главным маршрутизатором всегда будет становиться устройство с высоким приоритетом, даже при наличии в группе действующего главного маршрутизатора.

Резервный маршрутизатор с высоким приоритетом начинает отправлять объявления VRRP, в то время как главный маршрутизатор с низким приоритетом перестаёт отправлять их.

Форма **set** этой команды используется включения или выключения режима вытеснения.

Форма **delete** этой команды используется для установки значения по умолчанию.

Форма **show** используется для просмотра текущей настройки режима вытеснения.

23.2.4 interfaces <интерфейс> vrrp <идентификатор> preempt-delay <задержка>

Указание задержки осуществления вытеснения.

Синтаксис

```
set interfaces <интерфейс> vrrp <идентификатор> preempt-delay <задержка>
delete interfaces <интерфейс> vrrp <идентификатор> preempt-delay
show interfaces <интерфейс> vrrp <идентификатор> preempt-delay
```

Режим интерфейса

Режим настройки

Ветвь конфигурации

```
interfaces интерфейс {
   vrrp идентификатор {
      preempt-delay задержка
   }
}
```

Параметры

Интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны приведены в таблице в описании команды **interfaces <интерфейс> vrrp <идентификатор>**.

идентификатор

Числовой идентификатор виртуального маршрутизатора. Значение в диапазоне от 1 до 255.

задержка

Промежуток времени в секундах, на который происходит задержка вытеснения. Значения должны лежать в диапазоне 0-1000.

Значение по умолчанию

Задержка отсутствует.

Указания по использованию

Данная команда позволяет указать интервал времени ожидания перед началом вытеснения.

Форма **set** этой команды используется для указания задержки вытеснения.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** используется для просмотра текущего значения задержки вытеснения.

23.2.5 interfaces <интерфейс> vrrp <идентификатор> accept-mode <режим>

Приём пакетов устройством, не являющимся владельцем адреса.

Синтаксис

```
set interfaces <интерфейс> vrrp <идентификатор> accept-mode <режим>
delete interfaces <интерфейс> vrrp <идентификатор> accept-mode <режим>
show interfaces <интерфейс> vrrp <идентификатор> accept-mode <режим>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
   vrrp идентификатор {
      accept-mode режим
```

```
    }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны приведены в таблице в описании команды **interfaces <интерфейс> vrrp <идентификатор>**.

идентификатор

Числовой идентификатор виртуального маршрутизатора. Значение в диапазоне от 1 до 255.

режим

Необязательный. Допустимые значения:

true: Принимать пакеты (с учётом локального МЭ);

false: Игнорировать пакеты.

Значение по умолчанию

По умолчанию пакеты игнорируются.

Указания по использованию

Данная команда позволяет задать режим приёма пакетов с адресом назначения, совпадающим с VIP-адресом виртуального маршрутизатора. В случае значения true, пакеты будут обработаны с учётом правил межсетевого экрана, определённых для интерфейса. В случае значения false, пакеты будут проигнорированы. Команда справедлива для адресов, не являющихся собственными адресами интерфейса.

Форма **set** этой команды используется для указания режима приема пакетов устройством, не являющимся владельцем адреса.

Форма **delete** этой команды используется для установки значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего установленного значения.

23.2.6 interfaces <интерфейс> vrrp <идентификатор> unicast-peers <ipv4-адрес>

IP адреса назначения вместо группы многоадресной рассылки.

Синтаксис

```
set interfaces <интерфейс> vrrp <идентификатор> unicast-peers <ipv4-адрес>
delete interfaces <интерфейс> vrrp <идентификатор> unicast-peers
show interfaces <интерфейс> vrrp <идентификатор> unicast-peers
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
   vrrp идентификатор {
      unicast-peers ipv4-адрес
   }
}
```

Параметры

Интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны приведены в таблице в описании команды **interfaces <интерфейс> vrrp <идентификатор>**.

идентификатор

Числовой идентификатор виртуального маршрутизатора. Значение в диапазоне от 1 до 255.

<ipv4-адрес>

IP адрес, на который будут отправляться VRRP объявления.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать IP адрес, на который будет осуществлятся отправка VRRP объявлений. Если данный параметр не настроен, отправка производится с помощью многоадресной рассылки на адрес 224.0.0.18.

Поддерживается одновременная настройка нескольких значений IP адресов, при наличии 2 и более резервных маршрутизаторов.

Форма **set** этой команды используется для настройки отправки VRRP объявлений с помощью одноадресной рассылки.

Форма **delete** этой команды используется для удаления IP адреса одноадресной рассылки.

Форма **show** используется для просмотра текущей конфигурации IP адресов, используемых для одноадресной рассылки.

23.2.7 interfaces <интерфейс> vrrp <идентификатор> advertise-interval <интервал>

Установка интервала отправки объявлений VRRP.

Синтаксис

```
set interfaces <интерфейс> vrrp <идентификатор> advertise-interval <интервал>
delete interfaces <интерфейс> vrrp <идентификатор> advertise-interval
show interfaces <интерфейс> vrrp <идентификатор> advertise-interval
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
   vrrp идентификатор {
      advertise-interval интервал
   }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны приведены в таблице в описании команды **interfaces <интерфейс> vrrp <идентификатор>**.

идентификатор

Числовой идентификатор виртуального маршрутизатора. Значение в диапазоне от 1 до 255.

интервал

Необязательный. Интервал времени (в секундах) между отправкой объявлений VRRP. Параметр должен быть одинаковым для всех интерфейсов в рамках одного виртуального маршрутизатора. Значение лежит в диапазоне от 1 до 255. По умолчанию выставлено значение 1.

Значение по умолчанию

Главный маршрутизатор рассылает объявления VRRP с интервалом в одну секунду.

Указания по использованию

Данная команда позволяет задать интервал рассылки объявлений VRRP для заданного интерфейса.

Форма **set** этой команды используется для указания интервала рассылки объявлений VRRP в рамках виртуального маршрутизатора с данного интерфейса.

Форма **delete** этой команды используется для установки значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего установленного значения.

23.2.8 interfaces <интерфейс> vrrp <идентификатор> authentication password <пароль>

Установка пароля для виртуального маршрутизатора.

Синтаксис

```
set interfaces <интерфейс> vrrp <идентификатор> authentication password <пароль>

delete interfaces <интерфейс> vrrp <идентификатор> authentication password

show interfaces <интерфейс> vrrp <идентификатор> authentication password
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
    vrrp идентификатор {
        authentication {
            password пароль
        }
    }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны приведены в таблице в описании команды **interfaces <интерфейс> vrrp <идентификатор>**.

идентификатор

Числовой идентификатор виртуального маршрутизатора. Значение в диапазоне от 1 до 255.

пароль

Пароль, который будет использоваться интерфейсом для аутентификации на виртуальном маршрутизаторе (не более 8 символов).

Значение по умолчанию

По умолчанию пароль не задан.

Указания по использованию

Данная команда позволяет установить пароль для аутентификации на виртуальном маршрутизаторе.

ПРИМЕЧАНИЕ При установке пароля необходимо также указывать тип аутентификации. В противном случае система будет выдавать ошибку при попытке фиксации изменений (commit). При удалении пароля необходимо также удалить тип аутентификации.

Форма **set** этой команды используется для установки пароля для аутентификации на виртуальном маршрутизаторе.

Форма **delete** этой команды используется для удаления пароля.

Форма **show** этой команды используется для просмотра установленного пароля для аутентификации на виртуальном маршрутизаторе.

23.2.9 interfaces <интерфейс> vrrp <идентификатор> authentication type <тип>

Установка типа аутентификации для виртуального маршрутизатора.

Синтаксис

```
set interfaces <интерфейс> vrrp <идентификатор> authentication type <тип>
delete interfaces <интерфейс> vrrp <идентификатор> authentication type
show interfaces <интерфейс> vrrp <идентификатор> authentication type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
   vrrp идентификатор {
      authentication {
         type тип
      }
   }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны приведены в таблице в описании команды **interfaces <интерфейс> vrrp <идентификатор>**.

идентификатор

Числовой идентификатор виртуального маршрутизатора. Значение в диапазоне от 1 до 255.

тип

Тип аутентификации. Допустимые значения представлены ниже:

ah: Использование протокола IP Authentication Header (AH) для аутентификации;

plaintext-password: Использование текстового пароля.

Значение по умолчанию

Отсутствует. (По умолчанию аутентификация не требуется.)

Указания по использованию

Данная команда позволяет задать типа аутентификации на виртуальном маршрутизаторе.

ПРИМЕЧАНИЕ При установке типа аутентификации необходимо также указывать пароль. В противном случае система будет выдавать ошибку при попытке фиксации изменений (commit). При удалении типа аутентификации необходимо также удалить пароль.

Форма **set** этой команды используется для установки пароля для аутентификации на виртуальном маршрутизаторе.

Форма **delete** этой команды используется для удаления типа аутентификации.

Форма **show** этой команды используется для просмотра установленного типа аутентификации на виртуальном маршрутизаторе.

23.2.10 interfaces <интерфейс> vrrp <идентификатор> description <описание>

Указание текстового описания для виртуального маршрутизатора.

Синтаксис

```
set interfaces <интерфейс> vrrp <идентификатор> description <описание>
delete interfaces <интерфейс> vrrp <идентификатор> description
show interfaces <интерфейс> vrrp <идентификатор> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
    vrrp идентификатор {
        description описание
    }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны приведены в таблице в описании команды **interfaces <интерфейс> vrrp <идентификатор>**.

идентификатор

Числовой идентификатор виртуального маршрутизатора. Значение в диапазоне от 1 до 255.

описание

Краткое текстовое описание виртуального маршрутизатора. Если описание содержит пробелы, то оно должно быть заключено в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет задать текстовое описание виртуального маршрутизатора.

Форма **set** этой команды используется чтобы задать описание виртуального маршрутизатора.

Форма **delete** этой команды используется чтобы удалить описание виртуального маршрутизатора.

Форма **show** используется для просмотра описания виртуального маршрутизатора.

23.2.11 interfaces <интерфейс> vrrp <идентификатор> disable

Отключение виртуального маршрутизатора с сохранением существующей конфигурации.

Синтаксис

```
set interfaces <интерфейс> vrrp <идентификатор> disable
delete interfaces <интерфейс> vrrp <идентификатор> disable
show interfaces <интерфейс> vrrp <идентификатор>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
    vrrp идентификатор {
        disable
    }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны приведены в таблице в описании команды **interfaces <интерфейс> vrrp <идентификатор>**.

идентификатор

Числовой идентификатор виртуального маршрутизатора. Значение в диапазоне от 1 до 255.

Значение по умолчанию

Отсутствует (виртуальный маршрутизатор включен).

Указания по использованию

Данная команда используется для выключения виртуального маршрутизатора с заданным идентификатором в рамках указанного порта с сохранением его конфигурации.

Форма **set** этой команды используется для отключения виртуального маршрутизатора.

Форма **delete** этой команды используется для повторного включения виртуального маршрутизатора.

Форма **show** используется чтобы просмотра текущей конфигурации виртуального маршрутизатора.

23.2.12 interfaces <интерфейс> vrrp <идентификатор> hello-source-address <ipv4-адрес>

Указание источника пакетов анонса (advertisement messages) VRRP.

Синтаксис

```
set interfaces <интерфейс> vrrp <идентификатор> hello-source-address <ipv4-адрес>
delete interfaces <интерфейс> vrrp <идентификатор> hello-source-address
show interfaces <интерфейс> vrrp <идентификатор> hello-source-address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
   vrrp идентификатор {
      hello-source-address ipv4-адрес
   }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны приведены в таблице в описании команды **interfaces <интерфейс> vrrp <идентификатор>**.

идентификатор

Числовой идентификатор виртуального маршрутизатора. Значение в диапазоне от 1 до 255.

ipv4-адрес

IPv4-адрес сетевого интерфейса, входящего в состав виртуального маршрутизатора, который должен выступать в качестве источника пакетов VRRP обьявлений.

Значение по умолчанию

По умолчанию используется текущий IP-адрес, присвоенный интерфейсу.

Указания по использованию

Эта команда используется, чтобы указать адрес источника пакетов анонса (advertisement messages) VRRP, отличный от IP-адреса, присвоенного интерфейсу.

Форма **set** этой команды используется для указания IP-адреса источника пакетов анонса VRRP.

Форма **delete** этой команды используется для установки IP-адреса источника пакетов анонса VRRP, указанного по умолчанию.

Форма **show** используется для просмотра текущей настройки IP-адреса источника пакетов анонса VRRP.

23.2.13 interfaces <интерфейс> vrrp <идентификатор> strict-mode

Включение совместимости со стандартом RFC, указанным в узле version.

Синтаксис

```
set interfaces <интерфейс> vrrp <идентификатор> strict-mode
delete interfaces <интерфейс> vrrp <идентификатор> strict-mode
show interfaces <интерфейс> vrrp <идентификатор> strict-mode
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
   vrrp идентификатор {
      strict-mode
   }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны приведены в таблице в описании команды **interfaces <интерфейс> vrrp <идентификатор>**.

идентификатор

Числовой идентификатор виртуального маршрутизатора. Значение в диапазоне от 1 до 255.

Значение по умолчанию

Отсутствует (Режим совместимости со стандартом RFC отключен).

Указания по использованию

Данная команда, позволяет включить режим совместимости со стандартом RFC, указанным в узле version.

В данном режиме:

- отключается аутентификация
- отключается задержка вытеснения
- отключается accept-mode при использовании RFC 3768 (version 2)

Форма **set** этой команды используется для установки режима совместимости со стандартом RFC.

Форма **delete** этой команды используется для отключения режима совместимости со стандартом RFC.

Форма **show** используется для просмотра текущего значения конфигурации.

23.2.14 interfaces <интерфейс> vrrp <идентификатор> priority <приоритет>

Установка значения приоритета для маршрутизатора в рамках виртуального маршрутизатора.

Синтаксис

```
set interfaces <интерфейс> vrrp <идентификатор> priority <приоритет>
delete interfaces <интерфейс> vrrp <идентификатор> priority
show interfaces <интерфейс> vrrp <идентификатор> priority
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
   vrrp идентификатор {
      priority приоритет
   }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны приведены в таблице в описании команды **interfaces <интерфейс> vrrp <идентификатор>**.

идентификатор

Числовой идентификатор виртуального маршрутизатора. Значение в диапазоне от 1 до 255.

приоритет

Обязательный. Значение данного параметра определяет приоритет при выборе главного маршрутизатора в рамках виртуального маршрутизатора. Чем выше значение параметра, тем выше приоритет. Значение лежит в диапазоне от 1 до 254. Значение приоритета для главного маршрутизатора следует задавать из самого большого значения приоритета резервного маршрутизатора плюс 50. Значение приоритета 255 задаётся автоматически и только для владельца VIP-адреса.

Значение по умолчанию

По умолчанию приоритет маршрутизатора равен 100.

Указания по использованию

Данная команда, позволяет задать приоритет, исходя из которого выбирается главный маршрутизатор.

Форма **set** этой команды используется для указания значения приоритета.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** используется для просмотра текущего значения приоритета.

23.2.15 interfaces <интерфейс> vrrp <идентификатор> sync-group <имя_группы>

Добавление интерфейса в группу синхронизации.

Синтаксис

```
set interfaces <интерфейс> vrrp <идентификатор> sync-group <имя_группы>
delete interfaces <интерфейс> vrrp <идентификатор> sync-group
show interfaces <интерфейс> vrrp <идентификатор> sync-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
   vrrp идентификатор {
      sync-group имя_группы
```

```
    }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны приведены в таблице в описании команды **interfaces <интерфейс> vrrp <идентификатор>**.

идентификатор

Числовой идентификатор виртуального маршрутизатора. Значение в диапазоне от 1 до 255.

имя_группы

Название группы синхронизации.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет включить интерфейс в группу синхронизации.

Форма **set** этой команды используется для включения интерфейса в группу синхронизации.

Форма **delete** этой команды используется для удаления интерфейса из группы.

Форма **show** используется для просмотра текущей конфигурации синхронной группы для интерфейса.

23.2.16 interfaces <интерфейс> vrrp <идентификатор> version <версия_протокола>

Указание используемой версии протокола VRRP.

Синтаксис

```
set interfaces <интерфейс> vrrp <идентификатор> version <версия_протокола>
delete interfaces <интерфейс> vrrp <идентификатор> version
show interfaces <интерфейс> vrrp <идентификатор> version
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
   vrrp идентификатор {
      version версия_протокола
   }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны приведены в таблице в описании команды **interfaces <интерфейс> vrrp <идентификатор>**.

идентификатор

Числовой идентификатор виртуального маршрутизатора. Значение в диапазоне от 1 до 255.

версия_протокола

Значение используемой версии протокола VRRP. Допустимые значения представлены ниже:

2: Использование второй версии протокола VRRP;

3: Использование третьей версии протокола VRRP.

Значение по умолчанию

По умолчанию используется вторая версия протокола.

Указания по использованию

Данная команда позволяет задать используемую версию протокола VRRP для виртуального маршрутизатора.

Форма **set** этой команды используется для указания используемой версии протокола VRRP.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** используется для просмотра текущей версии протокола VRRP.

23.2.17 interfaces <интерфейс> vrrp <идентификатор> virtual-address <ipv4-адрес>

Указание VIP-адрес виртуального маршрутизатора группы VRRP.

Синтаксис

```
set interfaces <интерфейс> vrrp <идентификатор> virtual-address <ipv4-адрес>
delete interfaces <интерфейс> vrrp <идентификатор> virtual-address
show interfaces <интерфейс> vrrp <идентификатор> virtual-address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
   vrrp идентификатор {
      virtual-address ipv4-адрес
   }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны приведены в таблице в описании команды **interfaces <интерфейс> vrrp <идентификатор>**.

идентификатор

Числовой идентификатор виртуального маршрутизатора. Значение в диапазоне от 1 до 255.

ipv4_адрес

Обязательный. IPv4-адрес виртуального маршрутизатора.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет задать VIP-адрес для виртуального маршрутизатора.

Форма **set** этой команды используется для определения VIP-адреса.

Форма **delete** этой команды используется для удаления VIP-адреса.

Форма **show** используется для просмотра текущего VIP-адреса.

23.2.18 service vrrp restart

Перезапуск процесса VRRP.

Синтаксис

```
service vrrp restart
```

Режим команды

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для перезапуска процесса VRRP.

23.2.19 service vrrp show

Отображение информации о состоянии VRRP.

Синтаксис

```
service vrrp show [detail | interface <интерфейс> [vrid <идентификатор>] | statistics [interface <интерфейс> [vrid <идентификатор>]] | sync-group]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

detail

Отображает детальную информацию о состоянии VRRP.

interface

Отображает информацию о состоянии VRRP для заданного интерфейса.

vrid

Отображает информацию о состоянии VRRP для заданного виртуального маршрутизатора.

statistics

Отображает статистику VRRP.

sync-group

Отображает информацию о группе синхронизации VRRP.

интерфейс

Обязательный. Интерфейс на котором настроен VRRP.

идентификатор

Числовой идентификатор виртуального маршрутизатора. Значение в диапазоне от 1 до 255.

Значение по умолчанию

При отсутствии дополнительных параметров, команда отображает информацию о состоянии VRRP для всех интерфейсов, с настроенными параметрами VRRP.

Указания по использованию

Эта команда используется для вывода сведений о состоянии VRRP, включая информацию о выбранном главном маршрутизаторе и статистику.

23.2.20 show interfaces vrrp

Отображение информации о настроенных интерфейсах VRRP.

Синтаксис

```
show interfaces vrrp [detail | <идентификатор_vrrp_интерфейса> [brief]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

detail

Отображает детальную информацию о состоянии всех интерфейсов VRRP.

идентификатор_vrrp_интерфейса

Отображает информацию о состоянии указанного интерфейса VRRP.

brief

Отображает краткую информацию об указанном интерфейсе VRRP.

Значение по умолчанию

При отсутствии дополнительных параметров, команда отображает краткую информацию о состоянии для всех интерфейсов VRRP.

Указания по использованию

Эта команда используется для вывода сведений о состоянии интерфейса VRRP.

23.2.21 show interfaces vrrp <идентификатор_vrrp_интерфейса> capture

Отображение трафика на интерфейсе VRRP.

Синтаксис

```
show interfaces vrrp <идентификатор_vrrp_интерфейса> capture [port порт| not port порт]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

идентификатор_vrrp_интерфейса

Отображает информацию о состоянии указанного интерфейса VRRP.

port <порт>

Отображает трафик, проходящий через указанный порт интерфейса VRRP.

not port <порт>

Отображает трафик на всех портах интерфейса VRRP, за исключением указанного.

Значение по умолчанию

При отсутствии дополнительных параметров, команда отображает информацию о трафике, проходящем через все порты указанного интерфейса VRRP.

Указания по использованию

Эта команда используется для вывода сведений о трафике, проходящем через указанный интерфейс VRRP.

24 Сохранение состояние системы отслеживания при сбоях

24.1 Обзор реализации

Система отслеживания соединений, как и вся система Netfilter, находятся в ядре ОС, в контролируемой им области оперативной памяти хранится и актуальная информация о соединениях. Само ядро не занимается резервированием, но оно предоставляет средства для загрузки и выгрузки информации о соединениях «на лету», после чего остаётся только передавать эту информацию между системами кластера. Этой деятельностью вне ядра занимается служба conntrackd. В рамках конфигурации Numa Edge эта служба доступна как **conntrack-sync**, а кластерное ПО работает с ней через через агент **conntrack-failover**, реализованный в соответствии со стандартом LSB.

Упрощённо архитектура системы отслеживания соединений представлена на рисунке:

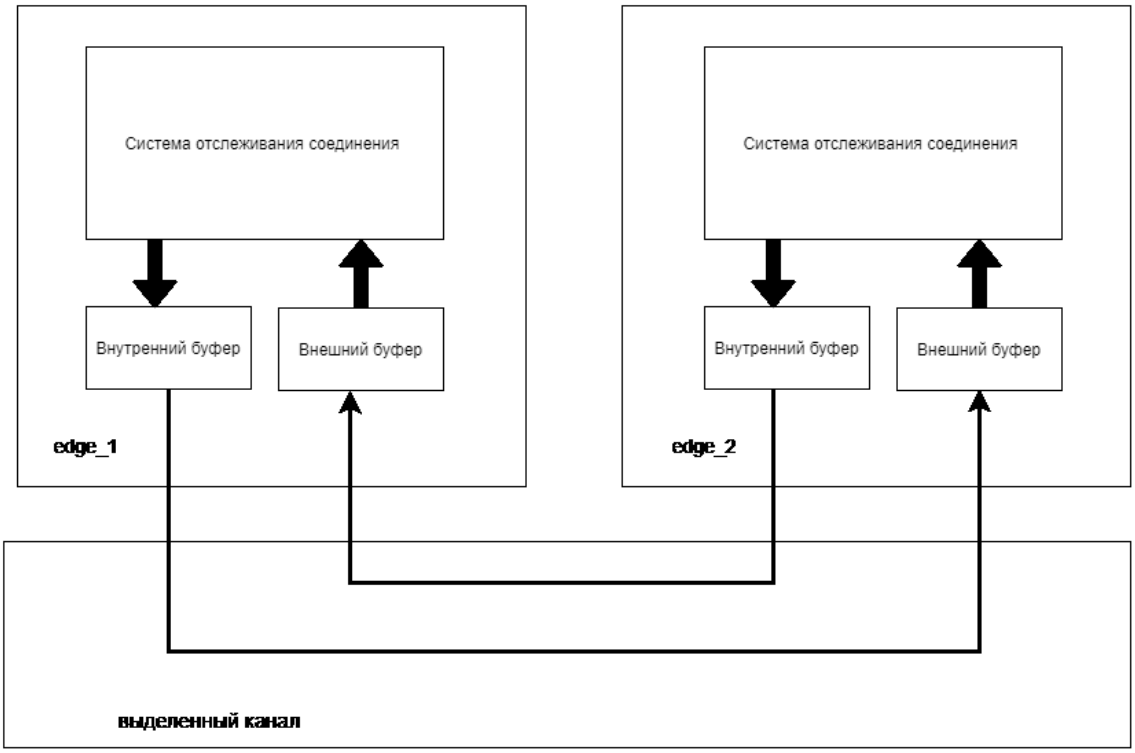


Рисунок 55 – Архитектура системы отслеживания соединений

Текущие изменения в информации о состоянии соединений сначала выгружаются во внутренний буфер, который поддерживается в той же системе, в которой эти изменения происходят. Затем изменения уже во внутреннем буфере копируются по сети в резервную систему, где попадают в её внешний буфер. В результате, с небольшой задержкой, у всех систем кластера оказывается актуальная информация о состоянии соединений, зафиксированных ведущей системой. В случае её краха, какая-то другая система кластера, ставшая ведущей, загружает информацию о соединениях из своего внешнего буфера в своё ядро и продолжает работу с соединениями примерно с момента краха предыдущей системы.

24.2 Ограничения текущей реализации

Из-за использования одних и тех же механизмов, но для разных целей, в общем случае нельзя одновременно управлять сохранением состояния соединений и использовать распараллеливание трафика по нескольким исходящим интерфейсам для «размазывания» нагрузки на каналы (WAN load balancing). В частности, очистка буферов в рамках управления или настройки системы отслеживания соединений вызовет сбой в работе системы распараллеливания трафика, которой учёт соединений нужен для выяснения фактической загруженности конкретного интерфейса (и, как следствие, канала, к которому этот интерфейс подключён).

24.3 Пример настройки

Для сохранения информации о соединениях службу **conntrack-sync** необходимо настроить и запустить в каждой системе, которую предполагается использовать для поддержки сохранения состояния соединений.

Ниже приведён пример настройки **conntrack-sync** для самостоятельной работы:

Пример 211 – пример настройки conntrack-sync для самостоятельной работы

Действие	**Команда**
Учитывать соединения через loopback интерфейс вряд ли необходимо, поэтому добавляем связанный с ним адрес в список игнорируемых.	`[edit]` `admin@edge# set service conntrack-sync address-ignore ipv4 127.0.0.1`
Эта сеть входит в общепринятый перечень сетей, выделенных для многоадресного вещания. Один адрес из неё используется в этом примере для общения служб **conntrack-sync** между собой, а следить за этими соединениями тоже необязательно.	`[edit]` `admin@edge# set service conntrack-sync address-ignore ipv4 226.0.0.0/24`
Задаём размер буфера (в байтах) для сообщений, которые **conntrackd** будет получать от системы отслеживания соединений ядра.	`[edit]` `admin@edge# set service conntrack-sync event-listen-queue-size 16777216`
Задаём сетевой интерфейс, через который службы **conntrack-sync** из разных систем будут обмениваться информацией о соединениях. Все такие интерфейсы должны быть включены в одну сеть.	`[edit]` `admin@edge# set service conntrack-sync interface eth2`
Задаём адрес назначения (идентификатор группы) для многоадресного вещания.	`[edit]` `admin@edge# set service conntrack-sync mcast-group 226.0.0.50`
Задаём размер приёмных и передающих буферов (в байтах), использующихся в обмене информацией о соединениях с другими службами **conntrack-sync**.	`[edit]` `admin@edge# set service conntrack-sync sync-queue-size 2097152`

Смотрим, что получилось.	`[edit]`
	`admin@edge# show service conntrack-sync`
	`+address-ignore {`
	`+ ipv4 127.0.0.1`
	`+ ipv4 226.0.0.0/24`
	`+}`
	`+event-listen-queue-size 16777216`
	`+interface eth2`
	`+mcast-group 226.0.0.50`
	`+sync-queue-size 2097152`
	
	`[edit]`
	
	`admin@edge01#`

Применение конфигурации.	`[edit]`
	`admin@edge# commit`
	`Starting conntrack-sync...`

При работе служб **conntrack-sync** данные о соединениях не применяются автоматически ведомой службой (например, через какой-то период времени), а только хранятся в её внешнем буфере. То есть нужно предпринимать какие-то дополнительные шаги для автоматизации этого процесса в контексте изменения внешних условий.

ПРИМЕЧАНИЕ Служба **conntrack-sync** сама по себе не отслеживает состояния соединений. Для отслеживания состояния соединений и их последующей синхронизации необходимо настроить правила фильтрации, основанные на состоянии соединений, либо правила трансляции сетевых адресов.

24.4 Система отслеживания соединений

Система отслеживания соединений является частью системы Netfilter, входящей в ядро, другими частями которой также являются системы фильтрации сетевых пакетов и преобразования сетевых адресов. Потребность в отслеживании соединений возникла из потребности принимать решения о фильтрации или преобразовании на основании не только данных из конкретного сетевого пакета, но и данных из предыдущих пакетов, как-то связанных с текущим. Олицетворением такой связи выбрана абстракция «соединение». К абстракциям с аналогичным названием в сетевых протоколах она прямого отношения не имеет, это только внутреннее представление ядром системы истории обмена пакетами между сетевыми узлами.

Соединение обладает параметром «состояние», значение которого определяется видами получаемых в рамках этого соединения пакетов и моментами их получения относительно друг друга. На данный момент поддерживаются следующие состояния соединений:

- **NEW**: новое соединение; полученный пакет является стартовым по правилам своего сетевого протокола и пакетный фильтр ещё не обнаружил ответного трафика, связанного с этим пакетом и участниками обмена, в рамках которого получен этот пакет;
- **ESTABLISHED**: установившееся соединение; соединение считается установившимся (установленным) когда пакетный фильтр обнаруживает ответный трафик, связанный с ранее обнаруженным исходным трафиком;
- **RELATED**: связанное соединение; для соединений с таким состоянием нужно учитывать ещё какое-то соединение, обмен в рамках которого и инициировал рассматриваемое (**RELATED**) соединение; хорошим примером соединения в состоянии **RELATED** является соединение для обмена данными (не управляющее) в пассивном режиме FTP;
- **INVALID**: ошибочное состояние; в рамках текущего соединения получены пакеты не того вида, который ожидался в данный момент по правилам выявленного в данном соединении протокола обмена.

В то время, как правила пакетного фильтра или преобразователя сетевых адресов являются статической информацией, которую можно оперативно восстановить из соответствующих конфигурационных файлов, информация о перечне распознанных соединений и их состоянии имеет динамический характер — она появляется в процессе реального обмена данными между сетевыми узлами и в общем случае уникальна.

Важность сохранения этой информации определяется её использованием в пакетном фильтре, правила которого, к примеру, могут предписывать устройству отбрасывать пакеты, не соответствующие текущему состоянию какого-то из соединений. В свою очередь, на выявление соединений влияют правила подсистемы преобразования адресов (поскольку они, например, позволяют изменять указанные в заголовках пакетов IP адреса отправителя или получателя данных).

В результате, в случае потери информации о соединениях на маршрутизаторе, установленном на границе сети, участникам обмена по обеим сторонам от него возможно (в зависимости от конфигурации пакетного фильтра и преобразователя адресов) придётся заново устанавливать соединения между собой.

При помощи устройств Numa Edge этой потери можно избежать благодаря использованию установленного в них инструментария **conntrack-tools** и организации кластера.

24.5 Краткие описания команд

Команды режима настройки	
service conntrack-sync address-ignore <версия_IP> <адрес>	Игнорирование сообщений системы отслеживания соединений про указанный адрес.
service conntrack-sync disable-external-cache	Отключение использования внешнего буфера
service conntrack-sync event-listen-queue-size <размер>	Установка размера буфера для сообщений от системы отслеживания соединений.
service conntrack-sync interface <имя_интерфейса>	Установка интерфейса, через который будет происходить обмен информацией о состоянии соединений.
service conntrack-sync mcast-group <адрес>	Установка адреса назначения для отправки информации о соединениях службам conntrack-sync в других системах.
service conntrack-sync netlink-reliable <состояние>	Включение режима получения сообщений от ядра без повторной синхронизации.

service conntrack-sync monitor-ip <адрес>	Установка виртуального адреса для переключения между активным и пассивным состоянием.
service conntrack-sync sync-queue-size <размер>	Установка размера буферов для сообщений о состоянии соединений от/для других служб conntrack-sync.
Эксплуатационные команды	
net connection-tracking clear	Очистка памяти ядра, содержащей информацию об отслеживаемых соединениях.
net connection-tracking show	Просмотр состояния отслеживаемых соединений.
service conntrack-sync clear external-cache	Очистка внешнего буфера и запрос актуальных данных у других систем.
service conntrack-sync clear internal-cache	Очистка внутреннего буфера, заполнение его информацией о текущем состоянии соединений в локальной системе и отправка этой новой информации службам conntrack-sync в других системах.
service conntrack-sync restart	Перезапуск службы conntrack-sync.
service conntrack-sync show	Вывод различных сведений о службе conntrack-sync

24.5.1 service conntrack-sync address-ignore <версия_IP> <адрес>

Игнорирование сообщений системы отслеживания соединений про указанный адрес.

Синтаксис

```
set service conntrack-sync address-ignore <версия_IP> <адрес>
delete service conntrack-sync address-ignore <версия_IP> <адрес>
show service conntrack-sync address-ignore <версия_IP> <адрес>
```

Режим команды

Режим настройки.

Ветвь конфигурации

```
service {
    conntrack-sync {
        address-ignore {
            версия_IP адрес
        }
    }
}
```

Параметры

версия_IP

Множественный узел. Версия межсетевого протокола (Internet Protocol — IP), по правилам которой приведён адрес системы или сети в следующем параметре. Допустимые форматы:

ipv4: Установить IPv4 адреса, для которых игнорируется трафик;

ipv6: Установить IPv6 адреса, для которых игнорируется трафик.

адрес

Множественный узел. Адрес системы или подсети, для которого следует игнорировать сообщения от системы отслеживания соединений. Указывается в соответствии с версией протокола IP, определенной в предыдущем параметре. Допустимые значения представлены в таблице ниже.

Таблица 212 – Форматы значений параметра адрес.

Значение	Описание
<x.x.x.x>	IPv4-адрес. Применим если параметр версия_IP установлен в значение ipv4.
<x.x.x.x/x>	IPv4-подсеть. Применим если параметр версия_IP установлен в значение ipv4.

<h:h:h:h:h:h:h:h>	IPv6-адрес. Применим если параметр версия_IP установлен в значение ipv6.
<h:h:h:h:h:h:h:h/x>	IPv6-подсеть. Применим если параметр версия_IP установлен в значение ipv6.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для указания адреса системы или сети, сообщения о которых от системы отслеживания соединений следует игнорировать. При этом адрес может относиться как к отправителю, так и к получателю. Эта команда полезна, когда необходимо уменьшить объёмы обрабатываемых и передаваемых данных о соединениях. Обычно можно игнорировать сообщения про адрес петлевого интерфейса (127.0.0.1), про IP-адреса, настроенные на самой системе (так как обычно интерес представляет проходящий, сквозной трафик) и про соединения в рамках адресного пространства многоадресной передачи (например, 224.0.0.0/24).

Форма **set** этой команды используется для указания адреса системы или сети, сообщения про которые от системы отслеживания соединений следует игнорировать.

Форма **delete** этой команды используется для восстановления приёма сообщений про указанный адрес системы или сети.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

24.5.2 service conntrack-sync disable-external-cache

Отключение использования внешнего буфера.

Синтаксис

```
set service conntrack-sync disable-external-cache
delete service conntrack-sync disable-external-cache
show service conntrack-sync
```

Режим команды

Режим настройки.

Ветвь конфигурации

```
service {
   conntrack-sync {
      disable-external-cache
   }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для отключения использования внешнего буфера.

Форма **set** этой команды используется для установки нужного значения параметра.

Форма **delete** этой команды используется для удаления параметру значения по умолчанию.

Форма **show** этой команды служит для просмотра текущего состояния конфигурации в этом контексте.

24.5.3 service conntrack-sync event-listen-queue-size <размер>

Установка размера буфера для сообщений от системы отслеживания соединений.

Синтаксис

```
set service conntrack-sync event-listen-queue-size <размер>
delete service conntrack-sync event-listen-queue-size
show service conntrack-sync event-listen-queue-size
```

Режим команды

Режим настройки.

Ветвь конфигурации

```
service {
    conntrack-sync {
        event-listen-queue-size размер
    }
}
```

Параметры

размер

Размер буфера в байтах. Значение должно лежать в диапазоне 0-4294967295.

Значение по умолчанию

По умолчанию размер буфера равен 8388608 байт (8 МБайт).

Указания по использованию

Эта команда предназначена для указания размера буфера, в который помещаются сообщения о соединениях от системы отслеживания соединений.

Если системный журнал наполняется сообщениями «**maximum netlink socket buffer size has been reached**», то размер буфера для сообщений следует увеличить.

Форма **set** этой команды используется для установки нужного значения параметра.

Форма **delete** этой команды используется для возвращения параметру значения по умолчанию.

Форма **show** этой команды служит для просмотра текущего состояния конфигурации в этом контексте.

24.5.4 service conntrack-sync interface <имя_интерфейса>

Установка интерфейса, через который будет происходить обмен информацией о состоянии соединений.

Синтаксис

```
set service conntrack-sync interface <интерфейс>
delete service conntrack-sync interface
show service conntrack-sync interface
```

Режим команды

Режим настройки.

Ветвь конфигурации

```
service {
    conntrack-sync {
        interface интерфейс
    }
}
```

Параметры

интерфейс

Обязательный параметр. Название сетевого интерфейса (например, **eth0**), через который должен производиться обмен информацией о состоянии соединений со службами conntrack-sync в других системах.

Значение по умолчанию

Отсутствует.

Указания по использованию

При работе conntrack-sync в рамках кластера стоит указывать здесь тот интерфейс, который используется кластерным ПО для обмена собственной информацией.

Форма **set** этой команды используется для установки нужного значения параметра.

Форма **delete** этой команды используется для стирания параметра из конфигурации службы.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

24.5.5 service conntrack-sync mcast-group <адрес>

Установка адреса назначения для отправки информации о соединениях службам conntrack-sync в других системах. Обмен производится посредством многоадресного вещания.

Синтаксис

```
set service conntrack-sync mcast-group <адрес>
delete service conntrack-sync mcast-group
show service conntrack-sync mcast-group
```

Режим команды

Режим настройки.

Ветвь конфигурации

```
service {
   conntrack-sync {
      mcast-group адрес
   }
}
```

Параметры

адрес

IPv4-адрес назначения многоадресной («multicast») передачи, используемый для рассылки информации о соединениях.

Значение по умолчанию

Значение адреса многоадресной передачи по умолчанию 225.0.0.50.

Указания по использованию

Указываемый в команде адрес не нужно связывать с каким-либо из сетевых интерфейсов системы.

Форма **set** этой команды используется для установки нужного значения параметра.

Форма **delete** этой команды используется для возвращения параметру значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

24.5.6 service conntrack-sync netlink-reliable <состояние>

Включение режима получения сообщений от ядра без повторной синхронизации.

Синтаксис

```
set service conntrack-sync netlink-reliable <состояние>
delete service conntrack-sync netlink
```

```
show service conntrack-sync netlink-reliable
```

Режим команды

Режим настройки.

Ветвь конфигурации

```
service {
   conntrack-sync {
      netlink-reliable on|off
   }
}
```

Параметры

состояние

Поддерживается одно из значений:

- **on** - включает режим с получением надежных сообщений
- **off** - включает режим с пересинхронизацией сообщений

Значение по умолчанию

По умолчанию установлено значение **on**.

Указания по использованию

По умолчанию используется режим с получением надежных сообщений от ядра. Для большинства сценариев использования рекомендуется использовать этот режим, однако при передаче объемов трафика близких к максимальной производительности лучшие результаты показывает режим с пересинхронизацией (**off**).

Форма **set** этой команды используется для установки нужного значения параметра.

Форма **delete** этой команды используется для возвращения параметру значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

24.5.7 service conntrack-sync monitor-ip <адрес>

Установка виртуального адреса для переключения между активным и пассивным состоянием.

Синтаксис

```
set service conntrack-sync monitor-ip <адрес>
delete service conntrack-sync monitor-ip <адрес>
show service conntrack-sync monitor-ip
```

Режим команды

Режим настройки.

Ветвь конфигурации

```
service {
   conntrack-sync {
      monitor-ip адрес
   }
}
```

Параметры

адрес

Формат – ipv4-адрес. Виртуальный адрес для переключения между состоянием.

Значение по умолчанию

Отсутствует.

Указания по использованию

Задает виртуальный адрес для переключения между активным и пассивным состоянием.

Форма **set** этой команды используется для установки нужного значения параметра.

Форма **delete** этой команды используется для возвращения параметру значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

24.5.8 service conntrack-sync sync-queue-size <размер>

Установка размера буфера для сообщений о синхронизации состоянии соединений от/для других служб conntrack-sync.

Синтаксис

```
set service conntrack-sync sync-queue-size <размер>
delete service conntrack-sync sync-queue-size
show service conntrack-sync sync-queue-size
```

Режим команды

Режим настройки.

Ветвь конфигурации

```
service {
   conntrack-sync {
      sync-queue-size размер
   }
}
```

Параметры

размер

Размер буфера в байтах. Оба буфера (и на приём, и на передачу) будут иметь такой — одинаковый — размер.

Значение по умолчанию

Значение по умолчанию равно 1048576 байт (1 МБайт).

Указания по использованию

Если в выводе команды **show conntrack-sync statistics** присутствует строка **“Lost msgs”**, то размер буфера следует увеличить.

Форма **set** этой команды используется для установки нужного значения параметра.

Форма **delete** этой команды используется для возвращения параметру значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

24.5.9 net connection-tracking clear

Очистка памяти ядра, содержащей информацию об отслеживаемых соединениях.

Синтаксис

```
clear connection-tracking
```

Режим команды

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для уничтожения имеющейся у ядра локальной системы информации о всех соединениях. После отдачи команды выдаётся запрос на подтверждение операции.

24.5.10 net connection-tracking show

Просмотр состояния отслеживаемых соединений.

Синтаксис

```
net connection-tracking show
```

Режим команды

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для просмотра состояния отслеживаемых соединений. Отслеживание состояний соединений может быть настроено в соответствующих политиках фильтрации, либо правилах трансляции сетевых адресов.

24.5.11 service conntrack-sync clear external-cache

Очистка внешнего буфера и запрос актуальных данных у других систем.

Синтаксис

```
service conntrack-sync clear external-cache
```

Режим команды

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для принудительной актуализации данных службы conntrack-sync в текущей системе до уровня данных служб conntrack-sync в других системах.

ПРИМЕЧАНИЕ: Во время выполнение команды очистки кеша, его состояние синхронизируется с таблицей состояния соединений ядра на основном устройстве.

24.5.12 service conntrack-sync clear internal-cache

Очистка внутреннего буфера, заполнение его информацией о текущем состоянии соединений в локальной системе и отправка этой новой информации службам conntrack-sync в других системах.

Синтаксис

```
service conntrack-sync clear internal-cache
```

Режим команды

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для принудительной очистки внутреннего буфера, заполнения его актуальной информацией о соединениях из ядра и отправки это актуальной информации службам conntrack-sync в других системах.

ПРИМЕЧАНИЕ: Во время выполнение команды очистки кеша, его состояние синхронизируется с таблицей состояния соединений ядра.

24.5.13 service conntrack-sync restart

Перезапуск службы conntrack-sync.

Синтаксис

```
service conntrack-sync restart
```

Режим команды

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для перезапуска службы conntrack-sync. После перезапуска служба заполнит внутренний буфер актуальными данными из ядра. Новое содержимое внутреннего буфера будет отправлено службам conntrack-sync в резервных системах для обновления их внешних буферов.

24.5.14 service conntrack-sync show

Вывод различных сведений о службе conntrack-sync.

Синтаксис

```
service conntrack-sync show [external-cache | internal-cache | statistics | status]
```

Режим команды

Эксплуатационный режим.

Параметры

external-cache

Отображение содержимого внешнего буфера службы conntrack-sync.

internal-cache

Отображение содержимого внутреннего буфера службы conntrack-sync.

statistics

Вывода статистических данных, относящихся к работе службы conntrack-sync.

status

Отображения информации о текущем состоянии службы conntrack-sync.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для отображения различных сведений о службе conntrack-sync.

25 Фильтрация и кеширования данных из web

25.1 Настройка веб-прокси

Настройка поведения посредника производится посредством отдачи поддерживаемых им команд через интерфейс командной строки либо через графический веб-интерфейс системы Numa Edge. Перечень поддерживаемых команд, их параметры и задаваемое ими поведение прокси рассмотрены ниже.

25.1.1 Примеры настройки фильтрации

На рисунке показана схема сети, на которой основаны приведённые ниже примеры. Предположим следующее:

- устройства из внутренней сети компании пользуются ресурсами Интернет через систему Numa Edge;
- фильтрация и кэширование веб-содержимого обеспечиваются веб-прокси, входящим в состав системы Numa Edge;
- веб-прокси не запущен, его конфигурация пуста.

Примеры сквозные, то есть учитывают друг друга. В самом первом из них настраивается привязка прокси к интерфейсу с адресом 192.168.1.254, после чего его (прокси) можно будет запустить (что и происходит по команде **commit**).

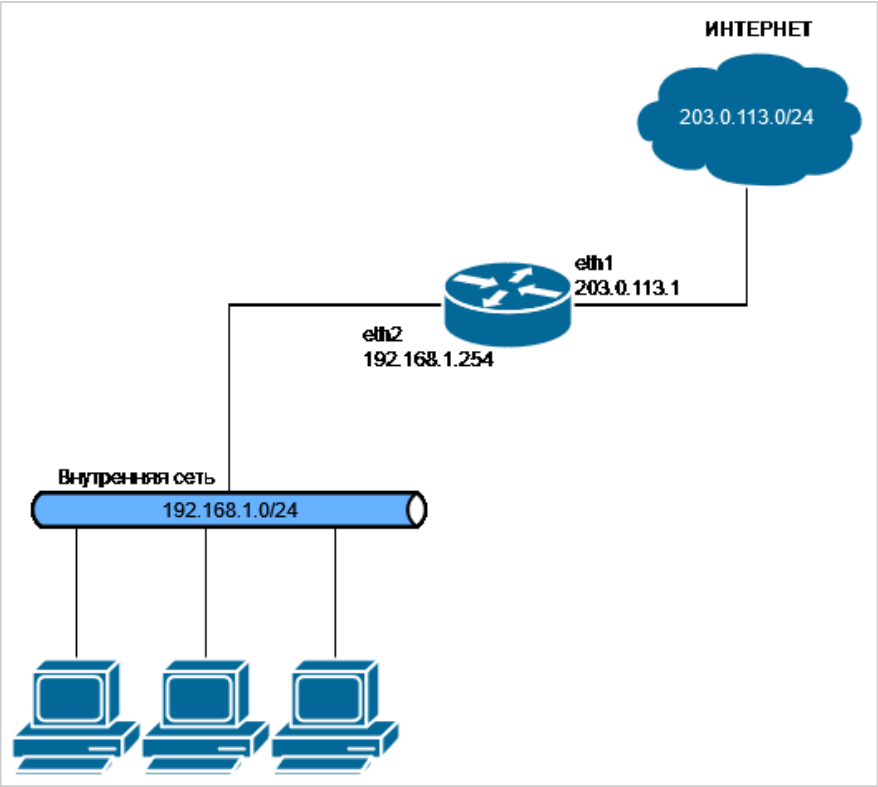


Рисунок 56 – Схема сети для примеров

В примерах этого раздела рассмотрены следующие ситуации:

- Настройка NAT
  - Настройка NAT для перенаправления HTTPS трафика на прокси сервер.
  - Настройка NAT для перенаправления HTTP трафика на прокси сервер.
  - Настройка NAT для маскировки адресов локальной сети
- Блокировка отдельных адресов (URL)
- Проверка работы фильтров
- Фильтрация по категории данных
- Фильтрация по ключевому слову
- Допуск к отдельным сайтам
- Перенаправление запросов пользователей

- Поддержка разных групп пользователей
- Учёт разных промежутков времени
- Работа с "белым" списком
- Настройка аутентификации пользователей на основе NTLM
- Настройка аутентификации пользователей на основе LDAP

Настройка NAT

В приведенной выше схеме видно, что Numa Edge будет использоваться на границе сети, поэтому необходимо настроить двунаправленное преобразование сетевых адресов (NAT masquerade). Помимо этого, вначале будет настроен прокси в "прозрачном" режиме и для его работы необходимо будет настроить перенаправление портов (DNAT) http и https на порты прокси 3128 и 3129, соответственно. Для работы прокси в "непрозрачном" режиме использование DNAT не требуется.

Настройка NAT для перенаправления HTTPS трафика на прокси сервер.

Пример 212 – Настройка правила 10 для ipv4 NAT

Действие	**Команда**
Создаем правило 10 для ipv4 NAT	`[edit]` `admin@edge#set service nat ipv4 rule 10`
Указываем, что данное правило будет использоваться для преобразования сетевого адреса и порта получателя	`[edit]` `admin@edge#set service nat ipv4 rule 10 type 'destination'`
Правило будет работать с пакетами, приходящими на интерфейс локальной сети (eth2)	`[edit]` `admin@edge#set service nat ipv4 rule 10 inbound-interface 'eth2'`
Указываем адрес, на который будут перенаправляться пакеты.	`[edit]` `admin@edge#set service nat ipv4 rule 10 inside-address address '192.168.1.254'`
Данное правило будет работать для протокола TCP. Это необходимый параметр для того, чтобы указать порт, на который будет перенаправляться трафик.	`[edit]` `admin@edge#set service nat ipv4 rule 10 protocol 'tcp'`
Перенаправляем https трафик	`[edit]` `admin@edge# set service nat ipv4 rule 10 destination port 'https'`
На порт 3129, который слушает прокси сервер.	`[edit]` `admin@edge#set service nat ipv4 rule 10 inside-address port '3129'`
Применяем текущие настройки	`[edit]` `admin@edge#commit`

Просмотр настроенного правила для NAT	`[edit]`
	`admin@edge# show service nat ipv4 rule 10`
	`destination {`
	`port https`
	`}`
	`inbound-interface eth2`
	`inside-address {`
	`address 192.168.1.254`
	`port 3129`
	`}`
	`protocol tcp`
	`type destination`

Настройка NAT для перенаправления HTTP трафика на прокси сервер.

Пример 213 – Настройка правила 20 для ipv4 NAT

Действие	**Команда**
Создаем правило 20 для ipv4 NAT	`[edit]` `admin@edge#set service nat ipv4 rule 20`

Указываем, что данное будет использоваться для преобразования сетевого адреса и порта получателя	[edit] admin@edge#set service nat ipv4 rule 20 type 'destination'
Правило будет работать с пакетами, приходящими на интерфейс локальной сети (eth2)	[edit] admin@edge#set service nat ipv4 rule 20 inbound-interface 'eth2'
Указываем адрес, на который будут перенаправляться пакеты.	[edit] admin@edge#set service nat ipv4 rule 20 inside-address address '192.168.1.254'
Данное правило будет работать для протокола TCP. Это необходимый параметр для того, чтобы указать порт, на который будет перенаправляться трафик.	[edit] admin@edge#set service nat ipv4 rule 20 protocol 'tcp'
Перенаправляем http трафик	[edit] admin@edge#set service nat ipv4 rule 20 destination port 'http'
На порт 3128, который слушает прокси сервер.	[edit] admin@edge#set service nat ipv4 rule 20 inside-address port '3128'
Применяем текущие настройки	[edit] admin@edge#commit

Просмотр настроенного правила для NAT	[edit]
	admin@edge# show service nat ipv4 rule 20
	destination {
	port http
	}
	inbound-interface eth2
	inside-address {
	address 192.168.1.254
	port 3128
	}
	protocol tcp
	type destination

Настройка NAT для маскировки адресов локальной сети

Пример 214– Настройка правила 30 для ipv4 NAT

Действие	**Команда**
Создаем правило 30 для ipv4 NAT	[edit] admin@edge# set service nat ipv4 rule 30
Указываем, что данное будет использоваться для двунаправленного преобразования сетевых адресов и портов	[edit] admin@edge# set service nat ipv4 rule 30 type 'masquerade'
Правило будет работать с пакетами, уходящими с WAN интерфейса (eth1)	[edit] admin@edge# set service nat ipv4 rule 30 outbound-interface 'eth1'
Применяем текущие настройки	[edit] admin@edge# commit
Просмотр настроенного правила для NAT	[edit] admin@edge# show service nat ipv4 rule 30 outbound-interface eth1 type masquerade

Настройка системного DNS сервера и службы кеширующего DNS

При установлении соединения с веб-сервером прокси-сервер получает информацию о доменном имени в заголовке "Host" протокола HTTP, либо поле SNI протокола TLS. Далее, прокси сервер самостоятельно получает значение IP адреса, соответствующее данному доменному имени, путем обращения с DNS-серверу. Ввиду этого необходимым требованием для корректной работы прокси-сервера является наличие настроенного системного DNS сервера. Также по соображениям безопасности и во исполнение требований RFC 2616 секции 14.23 значение IP адреса назначения HTTP/HTTPS пакета должно соответствовать заголовку Host/полю SNI. В

случае их несовпадения, прокси-сервер будет фиксировать в системном журнале предупреждение о данном несоответствии. Далее, в зависимости от значения атрибута **service webproxy host-verify-policy**:

- **strict(по умолчанию)** – соединение будет прервано, клиенту будет отправлен HTTP ответ с кодом 409;
- **warning** – соединение будет продолжено.

Во избежание данного поведения рекомендуется использовать либо общий кеширующий DNS сервер между клиентами и прокси-сервером, либо настроить на Numa Edge кеширующий DNS сервер. В этом примере производится настройка системного DNS сервера.

Пример 215 – Настройка системного DNS сервера

Действие	**Команда**
В качестве системного DNS сервера укажем IP-адрес Яндекс DNS.	[edit] admin@edge# set system dns name-server 77.88.8.8
Применение изменений.	[edit] admin@edge# commit

Просмотр получившейся конфигурации.	[edit]
	admin@edge# show system dns
	name-server 77.88.8.8 {
	}

Теперь необходимо настроить службу кеширующего DNS, который будет общаться к вышестоящему DNS серверу и кешировать ответы.

Пример 216 – Настройка службы кеширующего DNS

Действие	**Команда**
В качестве IP адреса, который будет слушать кеширующий DNS укажем адрес 192.168.1.254	[edit] admin@edge# set service dns forwarding listen-on address 192.168.1.254
Применение изменений.	[edit] admin@edge# commit

Просмотр получившейся конфигурации.	[edit]
	admin@edge# show service dns
	forwarding {
	listen-on {
	address 192.168.1.254
	}
	}
	[edit]

Блокировка сайтов без подмены сертификата

Данный пример описывает минимальные настройки для работы прокси сервера. Приводится конфигурация, которая позволяет блокировать доступ к домену vk.com, при открытии сайта через протокол HTTPS.

Пример 217– Запрет доступа к отдельным адресам

Действие	**Команда**
Включение ожидания запросов на интерфейсе с адресом 192.168.1.254.	[edit] admin@edge# set service webproxy listen-address 192.168.1.254
Включение поддержки фильтрации HTTPS трафика.	[edit] admin@edge# set service webproxy listen-address 192.168.1.254 enable-ssl
Блокировка доступа к домену vk.com с помощью анализа поля SNI в сообщении Client Hello.	[edit] admin@edge# set service webproxy url-filtering ssl block-server name vk.com

Действие	Команда
Применяем текущие настройки.	[edit] admin@edge# commit

Просмотр минимальной настройки прокси сервера.	[edit]
	admin@edge# show service webproxy
	listen-address 192.168.1.254 {
	enable-ssl
	}
	url-filtering {
	ssl {
	block-server {
	name vk.com
	}
	}
	}
	[edit]
	admin@edge#

Создание удостоверяющего центра

Создание удостоверяющего центра необходимо для генерации подменных сертификатов, при разрыве клиентского SSL соединения. В этом примере создается УЦ, который генерирует RSA сертификаты с длинной ключа 1024 байта.

Пример 218– Создание УЦ для генерации подменных сертификатов

Действие	Команда
Создание узла конфигурации удостоверяющего центра.	[edit] admin@edge# set pki ca WEB_PROXY_CA
Задание размера ключа, который будет использоваться в качестве ключевой пары для сертификата УЦ, и всех подписанным им сертификатов.	[edit] admin@edge# set pki ca WEB_PROXY_CA key-size 1024
В качестве типа ключа используется RSA.	[edit] admin@edge# set pki ca WEB_PROXY_CA key-type rsa
Срок действия сертификата удостоверяющего центра задается равным 5 годам.	[edit] admin@edge# set pki ca WEB_PROXY_CA expiration 1826
Для сертификата УЦ задается значение Common Name, указывающее его принадлежность.	[edit] admin@edge# set pki ca WEB_PROXY_CA cn "CA for WEB Proxy"
Применение конфигурации.	[edit] admin@edge# commit
Просмотр примененной конфигурации.	[edit] admin@edge# show pki ca WEB_PROXY_CA cn "CA for WEB Proxy" expires-on "Mon Jul 5 11:04:23 2027" key-size 1024 key-type rsa last-update "Tue Jul 5 11:04:23 2022" next-update "Mon Jul 5 11:04:23 2027" [edit] admin@edge#

Далее данный сертификат необходимо выгрузить из Numa Edge командой операционного режима.

Действие	Команда
Выход из конфигурационного режима в операционный.	[edit] admin@edge# exit
Экспорт сертификата УЦ в домашний каталог пользователя admin. Так же поддерживается	admin@edge:~$ pki export certificate WEB_PROXY_CA to /home/admin/

Действие	Команда
возможность экспорта на съемный носитель (без указания атрибута to), либо экспорт на удаленные узлы, используя протоколы SCP, FTP и TFTP.	Производится экспорт сертификата WEB_PROXY_CA в /home/admin/WEB_PROXY_CA.tgz Экспортируется сертификат WEB_PROXY_CA admin@edge-no-dm:~$

Сертификат будет экспортирован в архив, который будет необходимо распаковать и добавить в список доверенных УЦ на клиентских устройствах.

Включение подмены сертификатов для прокси-сервера

Данный пример описывает настройку прокси сервера для перехвата HTTPS соединений с последующей подменой сертификата веб сайта. Для этого необходимо описать домены, соединения к которым должно быть перехвачено. Далее необходимо указать сертификат УЦ, который будет генерировать подменные сертификаты веб-сайтов. Поскольку технология перехвата соединений включает в себя установку TLS соединения с требуемым веб-сервером со стороны Numa Edge, то на него необходимо импортировать корневые сертификаты доверенных УЦ. Обратите внимание, что если в процессе эксплуатации необходимо будет удалить один из корневых сертификатов УЦ, то после этого необходимо будет запустить службу webproxy, поскольку она кеширует сертификаты во внутреннем хранилище.

Пример 219– Включение функционала с подменой сертификатов

Действие	Команда
Переход в конфигурационный режим.	admin@edge-no-dm:~$ configure
Регулярное выражение обозначающее все возможные домены, где символ "." описывает любой символ, а символ "*" – любое количество повторений.	[edit] admin@edge# set service webproxy url-filtering ssl bump-server regex ".*"
В качестве УЦ, который будет генерировать подменяемые сертификаты указывается ранее созданный УЦ.	[edit] admin@edge# set service webproxy ssl x509-cert WEB_PROXY_CA
Применение конфигурации.	[edit] admin@edge# commit

ПРИМЕЧАНИЕ: Обратите внимание, что действия **ssl bump-server** и **ssl block-server** могут применяться одновременно, при этом блокировка является более приоритетным действием. В данном примере блокировка домена **vk.com** продолжает работать, несмотря на включение подмены сертификатов для всех доменов.

Блокировка отдельных адресов (URL)

Команды примера ниже при помощи фильтра **local-block** явно указывают отдельные адреса (вне категорий), запросы к которым будут блокироваться.

Пример 220– Запрет доступа к отдельным адресам

Действие	Команда
Запрет доступа к веб-сайту YouTube.	[edit] admin@edge# set service webproxy url-filtering squidguard local-block youtube.com
Запрет доступа к веб-сайту Facebook.	[edit] admin@edge# set service webproxy url-filtering squidguard local-block facebook.com
Применение изменений.	[edit] admin@edge# commit
Просмотр текущей конфигурации веб-прокси в этом контексте.	[edit] admin@edge# show service webproxy

	listen-address 192.168.1.254 {
	enable-ssl
	}
	ssl {
	x509-cert WEB_PROXY_CA
	}
	url-filtering {
	squidguard {
	local-block youtube.com
	local-block facebook.com
	}
	ssl {
	block-server {
	name vk.com
	}
	bump-server {
	regex ".*"
	}
	}
	}
	[edit]

Запрет доступа к веб-сайту YouTube.	[edit] admin@edge# set service webproxy url-filtering squidguard local-block youtube.com

Проверка работы фильтров

Проверить работу фильтров можно обращением с соответствующим запросом через веб-прокси к адресату в Интернет и последующим просмотром журнала событий в поисках свидетельства такого обращения. При этом должна быть включена запись информации о срабатывании фильтров в журналы (протоколирование).

Просмотреть содержимое журнала событий, например, по фильтру **local-block** из предыдущего примера, можно при помощи команды (запрещающие фильтры помещают адреса в так называемый "чёрный" список - blacklist).

Команда в примере ниже включает протоколирование запросов по адресам, закрытым фильтром **local-block** из предыдущего примера.

Пример 221– Включение протоколирования

Действие	**Команда**
Включение протоколирования всего, что перехватывается фильтром **local-block**. Параметр default добавляется автоматически для верхнеуровневых списков,так как могут иметь место и другие списки **local-block**, задаваемые в соответствии с правилами 'squidguard rule xxx' .	[edit] admin@edge# set service webproxy url-filtering squidguard log local-block-default
Применение изменений.	[edit] admin@edge# commit

Просмотр текущей конфигурации веб-прокси в этом контексте.	[edit]
	admin@edge# show service webproxy
	listen-address 192.168.1.254 {
	enable-ssl
	}
	ssl {
	x509-cert WEB_PROXY_CA
	}
	url-filtering {
	squidguard {
	local-block youtube.com
	local-block facebook.com
	log local-block-default
	}
	ssl {

Действие	Команда

	block-server {
	name vk.com
	}
	bump-server {
	regex ".*"
	}
	}

Фильтрация по категории данных

Команды из примера ниже включат блокирование адресов из заранее определённых в Numa Edge категорий "реклама" (**banner**), "шпионское ПО" (**spyware**) и "азартные игры" (**gambling**).

Пример 222– Включение фильтрации по категориям адресов

Действие	Команда
Включение блокирования адресов из категории "реклама".	[edit] admin@edge# set service webproxy url-filtering squidguard block-category banner
Включение блокирования адресов из категории "шпионское ПО".	[edit] admin@edge# set service webproxy url-filtering squidguard block-category spyware
Включение блокирования адресов из категории "азартные игры".	[edit] admin@edge# set service webproxy url-filtering squidguard block-category gambling
Применение изменений.	[edit] admin@edge# commit

Просмотр текущей конфигурации веб-прокси в этом контексте.	[edit]
	admin@edge# show service webproxy
	listen-address 192.168.1.254 {
	enable-ssl
	}
	ssl {
	x509-cert WEB_PROXY_CA
	}
	url-filtering {
	squidguard {
	block-category banner
	block-category spyware
	block-category gambling
	local-block youtube.com
	local-block facebook.com
	log local-block-default
	}
	ssl {
	block-server {
	name vk.com
	}
	bump-server {
	regex ".*"
	}
	}
	}

Фильтрация по ключевому слову

Команды из примера ниже запрещают доступ к сайтам, адреса которых содержат указанную последовательность символов. В этом примере блокируется доступ ко всем сайтам в доменной зоне Китая (".cn").

Пример 223– Включение фильтрации по ключевому слову

Действие	**Команда**
Запрет доступа ко всем сайтам доменной зоны Китая.	[edit] admin@edge# set service webproxy url-filtering squidguard local-block-keyword ".cn"
Применение изменений.	[edit] admin@edge# commit

Просмотр текущей конфигурации веб-прокси в этом контексте.	[edit]
	admin@edge# show service webproxy
	  listen-address 192.168.1.254 {
	  enable-ssl
	  }
	  ssl {
	  x509-cert WEB_PROXY_CA
	  }
	  url-filtering {
	  squidguard {
	  block-category banner
	  block-category spyware
	  block-category gambling
	  local-block youtube.com
	  local-block facebook.com
	  local-block-keyword ".cn"
	  log local-block-default
	  }
	  ssl {
	  block-server {
	  name vk.com
	  }
	  bump-server {
	  regex ".*"
	  }
	  }
	  }

Допуск к отдельным сайтам

Команды из примера ниже разрешают доступ к отдельным сайтам из заблокированных категорий. В этом примере открывается доступ к сайту по фиктивному адресу www.company-banner.com, хотя он (в рамках примера) числится в категории "реклама", доступ к сайтам из которой закрыт. Такое возможно благодаря тому, что приоритет фильтра **local-ok** выше приоритета фильтра **block-category** и соответствующее разрешающее действие сработает раньше запрещающего и тем самым остановит сверку.

Пример 224– Допуск к отдельным сайтам

Действие	**Команда**
Предоставление пользователям доступа к фиктивному сайту www.company-banner.com	[edit] admin@edge# set service webproxy url-filtering squidguard local-ok www.company-banner.com
Применение изменений.	[edit] admin@edge# commit

Просмотр текущей конфигурации веб-прокси в этом контексте.	[edit]
	admin@edge# show service webproxy
	  listen-address 192.168.1.254 {
	  enable-ssl
	  }
	  ssl {
	  x509-cert WEB_PROXY_CA
	  }
	  url-filtering {
	  squidguard {
	  block-category banner
	  block-category spyware
	  block-category gambling
	  local-block youtube.com
	  local-block facebook.com
	  local-block-keyword ".cn"
	  local-ok www.company-banner.com
	  log local-block-default
	  }
	  ssl {
	  block-server {
	  name vk.com
	  }
	  bump-server {
	  regex ".*"
	  }
	  }
	  }

Перенаправление запросов пользователей

По умолчанию, в ответ на запрос пользователя к заблокированному сайту возвращается страница другого, заранее определённого сайта. Адрес этой страницы задаётся при помощи команды **redirect-url**, также можно указать причину (по сути - категорию), по которой доступ по запрошенному пользователем адресу был закрыт. Команды из примера ниже указывают системе Numa Edge показывать страницу с категорией и адресом заблокированного сайта, к которому пытается обратиться пользователь.

Пример 225 - Установка адреса страницы с сайта-подмены для заблокированных адресов

Действие	**Команда**
Установка адреса нужной страницы. Приведённый в примере URL вызовет обращение. Этот скрипт вернёт страницу с заблокированным адресом и причиной, по которой доступ к URL был закрыт (обратите внимание на регистр символов в URL - в рамках HTTP он имеет значение).	[edit] admin@edge# set service webproxy url-filtering squidguard redirect-url "http://192.168.1.254/cgi-bin/squidGuard-simple.cgi?targetclass=%t&url=%u"
Применение изменений.	[edit] admin@edge# commit

Просмотр текущей конфигурации веб-прокси в этом контексте.	[edit]
	admin@edge# show service webproxy
	  listen-address 192.168.1.254 {
	  enable-ssl
	  }
	  ssl {
	  x509-cert WEB_PROXY_CA
	  }
	  url-filtering {
	  squidguard {
	  block-category banner
	  block-category spyware
	  block-category gambling
	  local-block youtube.com
	  local-block facebook.com
	  local-block-keyword ".cn"
	  local-ok www.company-banner.com7
	  log local-block-default
	  redirect-url
	http://192.168.1.254/cgi-bin/squidGuard-simple.cgitargetclass=%t&url=%u
	  }
	  ssl {
	  block-server {
	  name vk.com
	  }
	  bump-server {
	  regex ".*"
	  }
	  }
	  }

Поддержка разных групп пользователей

До этого момента во всех примерах подразумевалось, что все пользователи равноправны. Однако, при решении каких-то задач может возникнуть потребность обрабатывать запросы одних пользователей не так, как запросы других. Команда **source-group** позволяет сгруппировать пользователей по IP-адресам их систем, либо по адресам сетей, к которым относятся их системы. В примере 223 подразумевается та же схема сети, что и в примере 212, но сейчас она рассматривается как настроенная соответственно потребностями школы, где запросы системных администраторов, учителей и учащихся рассматриваются независимо.

Пример 226 – Настройка доступа в зависимости от группы

Действие	**Команда**
Очистка существующей конфигурации в отношении фильтрации запросов.	[edit] admin@edge# delete service webproxy url-filtering
Применение изменений.	[edit] admin@edge# commit
Регулярное выражение обозначающее все возможные домены, где символ "." описывает любой символ, а символ "*" – любое количество повторений.	[edit] admin@edge# set service webproxy url-filtering ssl bump-server regex ".*"
Возвращать в ответ на запросы к заблокированным сайтам титульную страницу сайта google.ru	[edit] admin@edge# set service webproxy url-filtering squidguard redirect-url "https://google.ru"
Создание группы для администраторов (с единственным IP-адресом).	[edit] admin@edge# set service webproxy url-filtering squidguard source-group ADMIN address 10.0.5.15
Создание группы для учителей (с одной подсетью).	[edit] admin@edge# set service webproxy url-

Действие	Команда
	`filtering squidguard source-group TEACHERS address 10.0.5.0/24`
Создание группы для учащихся (с первой из двух подсетей).	`[edit]` `admin@edge# set service webproxy url-filtering squidguard source-group STUDENTS address 10.0.1.0/24`
Создание группы для учащихся (со второй из двух подсетей).	`[edit]` `admin@edge# set service webproxy url-filtering squidguard source-group STUDENTS address 10.0.2.0/24`
Создание правила для фильтрации запросов от группы ADMIN. В данном случае ограничений нет.	`[edit]` `admin@edge# set service webproxy url-filtering squidguard rule 10 source-group ADMIN`
Создание правила для фильтрации запросов от группы TEACHERS.	`[edit]` `admin@edge# set service webproxy url-filtering squidguard rule 20 source-group TEACHERS`
Запрет доступа пользователей из группы TEACHERS к сайтам из категории “porn” ("сайты с порнографическим содержимым").	`[edit]` `admin@edge# set service webproxy url-filtering squidguard rule 20 block-category porn`
Запрет доступа пользователей из группы TEACHERS к сайтам из категории “shopping” ("сайты интернет-магазинов").	`[edit]` `admin@edge# set service webproxy url-filtering squidguard rule 20 block-category social-networks`
Создание правила для фильтрации запросов от группы STUDENTS.	`[edit]` `admin@edge# set service webproxy url-filtering squidguard rule 30 source-group STUDENTS`
Запрет доступа пользователей из группы STUDENTS к сайтам из категории “warez” ("краденое/взломанное ПО").	`[edit]` `admin@edge# set service webproxy url-filtering squidguard rule 30 block-category warez`
Запрет доступа пользователей из группы STUDENTS к сайтам из категории “drugs” ("наркотики").	`[edit]` `admin@edge# set service webproxy url-filtering squidguard rule 30 block-category drugs`
Запрет доступа пользователей из группы STUDENTS к сайтам из категории “filehosting” ("файлообмен").	`[edit]` `admin@edge# set service webproxy url-filtering squidguard rule 30 block-category filehosting`
Запрет доступа пользователей из группы STUDENTS к сайтам из категории “audio-video” ("аудио-видео содержимое").	`[edit]` `admin@edge# set service webproxy url-filtering squidguard rule 30 block-category audio-video`
Применение изменений.	`[edit]` `admin@edge# commit`

Просмотр текущей конфигурации веб-прокси в этом контексте.	`[edit]`
	`admin@edge# show service webproxy`
	`  listen-address 192.168.1.254 {`
	`  enable-ssl`
	`  }`
	`  ssl {`
	`  x509-cert WEB_PROXY_CA`
	`  }`
	`  url-filtering {`
	`  squidguard {`
	`  redirect-url https://google.ru`

Действие	Команда

	rule 10 {
	source-group ADMIN
	}
	rule 20 {
	block-category porn
	block-category social-networks
	source-group TEACHERS
	}
	rule 30 {
	block-category warez
	block-category drugs
	block-category filehosting
	block-category audio-video
	source-group STUDENTS
	}
	source-group ADMIN {
	address 10.0.5.15
	}
	source-group STUDENTS {
	address 10.0.1.0/24
	address 10.0.2.0/24
	}
	source-group TEACHERS {
	address 10.0.5.0/24
	}
	}
	ssl {
	bump-server {
	regex ".*"
	}
	}
	}

Учёт разных промежутков времени

В предыдущем примере правила фильтрации применялись независимо от момента времени. Для привязки связанных с группой правил фильтрации к промежуткам времени вроде будних дней и времени суток применяется команда time-period.

Команды из примера 227 подразумевают пример 226 и показывают, как добавить в правила фильтрации учёт временных промежутков. В этом примере вводится новое правило с номером 25, в котором пользователям из группы TEACHERS закрывается доступ к сайтам из категории «porn» во внеучебное время (временной интервал AFTERHOURS), при этом остальные категории не блокируются. Вместе с тем существующее правило 20 дополняется временным промежутком SCHOOLHOURS, благодаря чему оно актуально только в учебные часы. В результате получается, что в учебные часы у пользователей группы TEACHERS закрыт доступ к сайтам из категорий «porn» и «shopping», а во внеучебные - только к «porn».

Пример 227 – Применение правил в определённое время суток

Действие	Команда
Определение временного периода под названием SCHOOLHOURS, обозначающего рабочие (учебные) часы.	[edit] admin@edge# set service webproxy url-filtering squidguard time-period SCHOOLHOURS day workday time "09:00-12:00,13:00-16:00"
Определение временного периода под названием AFTERHOURS, обозначающего нерабочее время.	[edit] admin@edge# set service webproxy url-filtering squidguard time-period AFTERHOURS day weekend time "00:00-24:00" [edit] admin@edge# set service webproxy url-filtering squidguard time-period

Действие	**Команда**
	AFTERHOURS day workday time "00:00-19:00, 12:00-13:00, 16:00-00:00"
Уточнение правила 20 этим промежутком времени - теперь оно актуально только во время учебных часов.	[edit] admin@edge# set service webproxy url-filtering squidguard rule 20 time-period SCHOOLHOURS
Создание нового правила для фильтрации запросов от группы TEACHERS ("преподаватели") во внеучебное время.	[edit] admin@edge# set service webproxy url-filtering squidguard rule 25 source-group TEACHERS
Правило 25 актуально только во внеучебное время.	[edit] admin@edge# set service webproxy url-filtering squidguard rule 25 time-period AFTERHOURS
Закрытие доступа пользователей из группы TEACHERS к сайтам только из категории “porn”.	[edit] admin@edge# set service webproxy url-filtering squidguard rule 25 block-category porn
Применение изменений.	[edit] admin@edge# commit

Просмотр текущей конфигурации веб-прокси в этом контексте.	[edit]
	admin@edge# show service webproxy
	  listen-address 192.168.1.254 {
	  enable-ssl
	  }
	  ssl {
	  x509-cert WEB_PROXY_CA
	  }
	  url-filtering {
	  squidguard {
	  redirect-url https://google.ru
	  rule 10 {
	  source-group ADMIN
	  }
	  rule 20 {
	  block-category porn
	  block-category social-networks
	  source-group TEACHERS
	  time-period SCHOOLHOURS
	  }
	
	  rule 25 {
	  block-category porn
	  source-group TEACHERS
	  time-period AFTERHOURS
	  }
	  rule 30 {
	  block-category warez
	  block-category drugs
	  block-category filehosting
	  block-category audio-video
	  source-group STUDENTS
	  }
	  source-group ADMIN {
	  address 10.0.5.15
	  }
	  source-group STUDENTS {
	  address 10.0.1.0/24
	  address 10.0.2.0/24
	  }

Действие	Команда

	source-group TEACHERS {
	address 10.0.5.0/24
	}
	time-period AFTERHOURS {
	day workday {
	time "00:00-19:00, 12:00-13:00, 16:00-00:00"
	}
	day weekend {
	time 00:00-24:00
	}
	}
	time-period SCHOOLHOURS {
	day workday {
	time "09:00-12:00, 13:00-16:00"
	}
	}
	}
	ssl {
	bump-server {
	regex ".*"
	}
	}
	}

Работа с "белым" списком

Распространённым способом фильтрации веб-содержимого является предоставление доступа ко всем сайтам за исключением некоторых заблокированных (составляющих, таким образом, "чёрный" список). Однако, бывают ситуации, когда необходимо, наоборот, закрыть доступ ко всем сайтам за исключением некоторых разрешённых (составляющих "белый" список). В примере ниже показано создание "белого" списка.

Пример 228 – Определение "белого" списка

Действие	Команда
Очистка существующей конфигурации.	[edit] admin@edge# delete service webproxy url-filtering
Применение изменений.	[edit] admin@edge# commit
Регулярное выражение обозначающее все возможные домены, где символ "." описывает любой символ, а символ "*" – любое количество повторений.	[edit] admin@edge# set service webproxy url-filtering ssl bump-server regex ".*"
Возвращать в ответ на запросы к заблокированным сайтам титульную страницу сайта google.ru.	[edit] admin@edge# set service webproxy url-filtering squidguard redirect-url "https://google.ru"
Запрещение доступа ко всем сайтам в качестве действия по умолчанию (т.е. если явно не указано иное).	[edit] admin@edge# set service webproxy url-filtering squidguard default-action block
Разрешение доступа к сайту “numatech.ru”.	[edit] admin@edge# set service webproxy url-filtering squidguard local-ok numatech.ru
Разрешение доступа к сайту “yandex.ru”.	[edit] admin@edge# set service webproxy url-filtering squidguard local-ok yandex.ru
Разрешение доступа к сайту “google.ru”.	[edit] admin@edge# set service webproxy url-filtering squidguard local-ok google.ru

Действие	Команда
Применение изменений.	[edit] admin@edge# commit

Просмотр текущей конфигурации веб-прокси в этом контексте.	[edit]
	admin@edge# show service webproxy
	listen-address 192.168.1.254 {
	enable-ssl
	}
	ssl {
	x509-cert WEB_PROXY_CA
	}
	url-filtering {
	squidguard {
	default-action block
	local-ok numatech.ru
	local-ok yandex.ru
	local-ok google.ru
	redirect-url https://google.ru
	}
	}
	ssl {
	bump-server {
	regex ".*"
	}
	}
	}

Настройка аутентификации пользователей на основе NTLM

В примере ниже приведена настройка аутентификации пользователей прокси-сервера на основе NTLM. На рисунке приведена используемая схема сети.

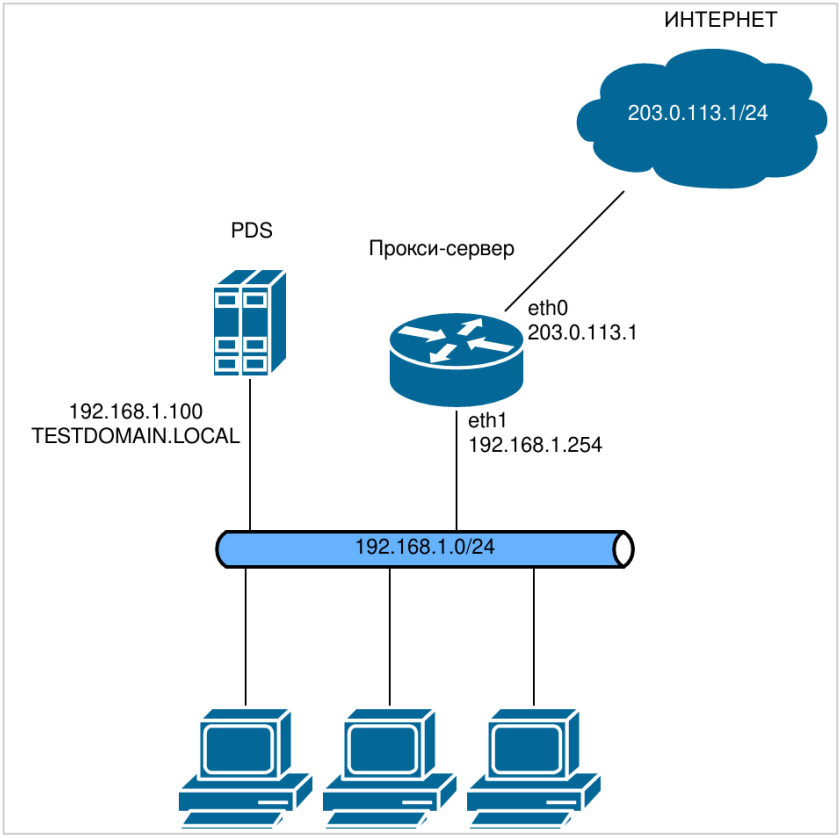


Рисунок 57 – Аутентификация пользователей прокси на основе протокола NTLM

Для корректной работы аутентификации на основе NTLM должны быть выполнены следующие условия:

- Настройка клиентской машины:
- Пользователь должен быть членом домена и находится в базе данных контроллера домена Microsoft Active Directory. Компьютер клиента должен находиться в базе контроллера домена.
- В настройках прокси веб-обозревателя должно быть установлено полное доменное имя (FQDN) прокси-сервера (или IP-адрес) и номер порта (например, 3128).
- Настройка сервера Microsoft Active Directory:
- Должен быть настроен сервер Active Directory.
- Должен быть настроен сервер DNS. На сервере DNS должна быть создана запись с доменным именем прокси-сервера.
- В домене необходимо создать учетную запись для прокси-сервера с правами на ввод компьютеров в домен.
- В данном примере предполагается следующее:
- На компьютере под управлением Windows, являющимся PDC, настроен домен TESTDOMAIN.LOCAL.
- В настройке сервера DNS создана запись с доменным именем для прокси-сервера edge.testdomain.local.
- PDC имеет IP-адрес 192.168.1.100.
- В базе AD создана учетная запись для прокси-сервера с правами администратора.

Помимо этого необходимо удалить настройки перенаправления http и https трафика, настроенные ранее, для работы прокси в "прозрачном" режиме.

Для настройки аутентификации пользователей прокси на основе NTLM, необходимо выполнить следующие шаги в режиме настройки:

Пример 229 – Удаление настроенных выше правил для "прозрачного" режима

Действие	**Команда**
Удаление перенаправления https трафика на порт 3129	`[edit]` `admin@edge#set service nat ipv4 rule 10`
Удаление перенаправления http трафика на порт 3128	`[edit]` `admin@edge#set service nat ipv4 rule 20`
Применение изменений.	`[edit]` `admin@edge# commit`

Пример 230 – Настройка аутентификации пользователей прокси на основе NTLM

Действие	**Команда**
Отключение "прозрачного" режима работы прокси-сервера.	`[edit]` `admin@edge# set service webproxy listen-address 192.168.1.254 disable-transparent`
Установка аутентификации клиентов на основе NTLM.	`[edit]` `admin@edge# set service webproxy authentication method ntlm`
Указание имени компьютера в домене.	`[edit]` `admin@edge# set service webproxy authentication ntlm name edge`
Указание пароля для учетной записи, созданной в AD для прокси сервера.	`[edit]` `admin@edge# set service webproxy authentication ntlm password 123`
Указание адреса контроллера домена.	`[edit]` `admin@edge# set service webproxy authentication ntlm pdc 192.168.1.100`
Указание имени пользователя.	`[edit]` `admin@edge# set service webproxy authentication ntlm user proxy`
Указание имени домена.	`[edit]` `admin@edge# set service webproxy authentication ntlm workgroup testdomain`
Фиксация конфигурации.	`[edit]` `admin@edge# commit`

Настройка аутентификации пользователей на основе LDAP

Numa Edge поддерживает возможность проверки подлинности клиентов прокси с использованием службы каталогов на основе протокола LDAP. Для этого необходимо настроить параметры подключения к серверу LDAP, для этого используется ветвь конфигурации system ldap-server.

При использовании аутентификации пользователей возможна работа только в непрозрачном режиме прокси, при этом на клиентском ПО должны быть соответствующим образом прописаны настройки прокси-сервера.

При использовании аутентификации на основе LDAP, пользователю выдается приглашение на ввод регистрационного имени и пароля.

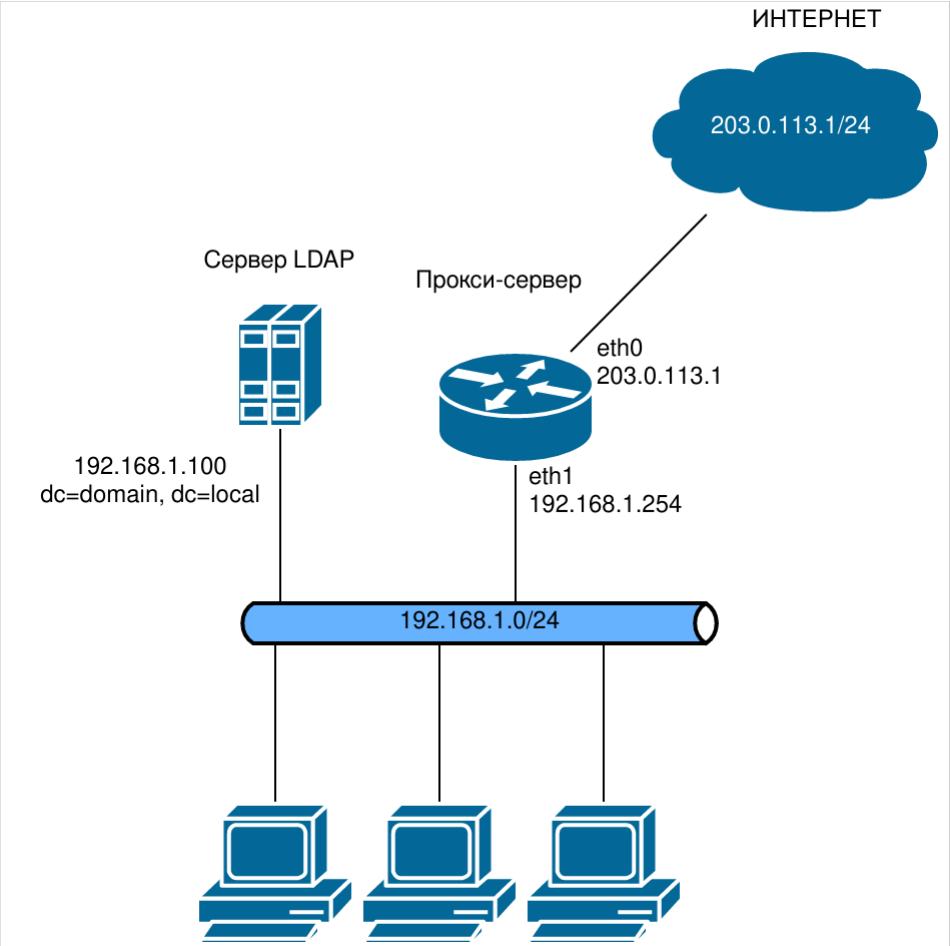


Рисунок 58 – Аутентификация пользователей прокси на основе протокола LDAP

В примере ниже приведена настройка параметров подключения к серверу LDAP.

Пример 231– Настройка параметров подключения к серверу LDAP

Действие	Команда
Указание имени привязки, используемого для подключения к серверу LDAP.	`[edit]` `admin@edge# set system ldap-server dn cn=edgeproxy,dc=domain,dc=local`
Указание IP-адреса сервера LDAP.	`[edit]` `admin@edge# set system ldap-server host 192.168.1.100`
Указание базового DN, в котором будет осуществляться поиск.	`[edit]` `admin@edge# set system ldap-server basedn dc=domain,dc=local`
Указание пароля для аутентификации на сервере LDAP.	`[edit]` `admin@edge# set system ldap-server password testpassword`
Указание используемого для подключения к	`[edit]`

Действие	Команда
серверу LDAP номера сетевого порта.	admin@edge# set system ldap-server port 389
Указание корневого объекта каталога, начиная от которого необходимо производить поиск учетных записей пользователей.	[edit] admin@edge# set system ldap-server userbasedn cn=edgeproxy,dc= domain,dc=local
Указание корневого объекта каталога, начиная от которого необходимо производить поиск учетных записей пользователей	[edit] admin@edge# set system ldap-server groupbasedn cn=groups,dc= domain,dc=local
Фиксация конфигурации.	[edit] admin@edge# commit

В примере ниже приведена настройка параметров прокси-сервера для включения аутентификации на основе протокола LDAP.

Пример 232 – Включение аутентификации на основе LDAP в параметрах прокси-сервера

Действие	Команда
Указание аутентификации на основе LDAP.	[edit] admin@edge#set service webproxy authentication method ldap
Отключение прозрачного режима.	[edit] admin@edge#set service webproxy listen-address 192.168.1.254 disable-transparent
Фиксация конфигурации.	[edit] admin@edge# commit

25.2 Потребление оперативной памяти

При работе в любом режиме объем занимаемой прокси-сервером оперативной памяти делится на две части: статическую часть (резервируется независимо от настроек) и зависимую часть (зависит от настроек дискового кэша).

В связи с архитектурными особенностями статическая часть представляет собой совокупность кэша оперативной памяти и зарезервированного пространства оперативной памяти (75 МБ) на каждое процессорное ядро. Зависимая часть определяется как количество записей, умноженное на заданное значение дискового кэша.

По умолчанию в прокси-сервере поддержка дискового кэша не настроена. Если включить данную поддержку, то объем потребляемой прокси-сервером оперативной памяти будет прямопропорционально зависеть от заданного значения дискового кэша.

Таким образом, объем потребляемой прокси-сервером оперативной памяти определяется по следующей формуле:

(75×N+R)+(D×0.003), где:

N — количесво процессоров;

R — кэш оперативной памяти (256 МБ);

D — дисковый кэш (МБ).

Например, пусть количество процессоров равно двум, объем дискового кэша равен 200 ГБ (204800 МБ), тогда получаем следующее выражение для расчета потребляемой оперативной памяти прокси-сервером:

(75×2+256)+(204800×0,003)=1020,4 (МБ)

Таким образом, для того, чтобы прокси-сервер потреблял меньше оперативной памяти, рекомендуется задавать небольшое значение дискового кэша.

25.3 Режимы работы веб-прокси

Посредник может работать в нескольких режимах, которые можно комбинировать для решения разных задач. По контексту применения выделяются следующие режимы:

- взаимодействия с клиентским ПО (например, веб-браузерами пользователей): "прозрачный" и "непрозрачный";
- аутентификации пользователей прокси: без аутентификации, с аутентификацией на основе LDAP, с аутентификацией на основе NTLM;
- обработки запросов пользователей (URL содержимого, IP-адрес источника и так далее): с фильтрацией и без фильтрации;
- обработки полученного в ответ на запросы пользователей веб-содержимого: с кэшированием и без кэширования;
- с включенным и отключенным режимом проксирования SSL.

25.3.1 Кэширование ответов на запросы пользователей

Основная задача прокси - изоляция одной (защищаемой) сети от другой (публичной). Достигается это исключением "прямых" соединений между клиентами из защищаемой сети и их адресатами из публичной. Вместо этого клиент (клиентское ПО) обращается к посреднику с просьбой загрузить для него (клиента) что-либо из публичной сети по указанному клиентом URL (при "непрозрачной" работе прокси). При работе в "прозрачном" режиме посредник делает это сам, имитируя для клиента "прямое" соединение. В результате в распоряжении посредника оказывается веб-содержимое, запрошенное клиентом. Современное веб-пространство устроено так, что значительная доля содержимого изменяется довольно редко или вообще не изменяется, поэтому разумно наделить посредника способностями выявлять такое содержимое, сохранять его у себя и впредь, в ответ на соответствующие запросы клиентов, отдавать сохранённую у себя копию запрошенного содержимого, не обращаясь за ним к адресату в Интернет.

Такая деятельность посредника называется кэшированием, а его хранилище копий содержимого - кэшем. Разумеется, предусмотрены и рычаги управления кэшированием, они 4описаны ниже в этой главе.

По умолчанию в системе Numa Edge кэширование средствами веб-прокси выключено.

ПРИМЕЧАНИЕ Не рекомендуется включать кэширование веб-содержимого в системах, использующих в качестве устройства хранения флэш-накопители. Кэширование веб-содержимого вызывает частые операции записи данных на носитель, что сильно сокращает срок службы флэш-накопителя. Кэширование веб-содержимого должно включаться только в системах с "обычными" жёсткими дисками.

25.3.2 Фильтрация запросов пользователей

Поскольку посредник анализирует и исполняет запросы пользователей, то есть возможность управлять его поведением в зависимости от того что, откуда и когда запрашивается. Можно настроить реакцию на определённые доменные имена, IP-адреса, типы MIME, символьные комбинации в пределах URL и так далее. В ответ на "неподходящий" запрос клиента можно вместо запрошенного содержимого отдавать как собственные страницы с разным содержимым (например, с сообщениями вроде "Доступ запрещён"), так и страницы с других ресурсов (здесь это называется "перенаправление"). Также есть возможность настроить поведение посредника в зависимости от информации об источнике запроса (например, IP-адреса системы клиента) и текущей ситуации (скажем, времени суток).

По умолчанию в системе Numa Edge фильтрация средствами веб-прокси выключена, все запросы пропускаются беспрепятственно.

Порядок фильтрации запросов пользователей

Фильтрация запросов пользователей производится посредником Numa Edge на основе фильтров, которые могут существовать "сами по себе", в качестве глобальных фильтров, и внутри частных (уточняющих) правил фильтрации. При получении запроса от пользователя прокси сверяет имеющиеся в этом запросе данные (URL адресата, IP-адрес источника и так далее) с соответствующими данными в правилах и глобальных фильтрах на предмет совпадения или попадания в диапазон. Если это происходит, то правило или глобальный фильтр "применяются" - прокси выполняет указанное в них действие, например, отказывает в исполнении запроса или, наоборот, исполняет его в качестве исключения.

Сначала производится сверка с правилами, до первого совпадения или попадания в диапазон. Если правила применить не получилось, то производится сверка с глобальными фильтрами, тоже до первого совпадения или попадания в диапазон. Если и глобальные фильтры применить не получилось, то прокси выполняет действие по умолчанию, задаваемое командой .

Порядок перебора правил определяется их номерами - от 1 до 1024, по возрастанию. Порядок перебора фильтров (как внутри правил, так и глобальных) определяется их приоритетом - фильтр с высшим приоритетом сверяется первым. Ниже приведён перечень фильтров (без параметров и команд) в соответствии с их приоритетами (1 — высший):

- **local-ok** - разрешает доступ к указанному адресу IP или домену;
- **local-block** - запрещает доступ к указанному адресу IP или домену;
- **allow-ipaddr-url** - разрешает запросы, в URL которых вместо доменного имени сайта указан IP-адрес;
- **block-category** - запрещает доступ по адресам из указанной категории;
- **allow-category** - разрешает доступ по адресам из указанной категории;
- **local-block-keyword** - блокирует запросы к содержимому, URL которого содержит указанный набор символов;
- **local-block-url** – блокирует доступ к указанному URL;
- **local-ok-url** – разрешает доступ к указанному URL
- **default-action** - задаёт действие, которое будет применяться ко всем запросам, не попавшим под имеющиеся фильтры (и глобальные, и в правилах).

Правила предназначены для сужения области применения фильтров за счёт наложения дополнительных условий. В качестве этих условий выступают промежутки времени и информация об источнике запроса. В этом случае фильтры применяются только тогда, когда соблюдаются все указанные в правиле дополнительные условия (например, текущее время попадает в указанный в условии диапазон).

25.3.3 Проксирование соединений SSL

Фильтрация данных, доступ к которым осуществляется через установление SSL соединений (по HTTPS), осуществляется с помощью двух способов.

- Без разрыва SSL соединения с помощью анализа поля SNI (Server Name Indication). Настройка данного режима работы осуществляется с помощью атрибута **set service webproxy url-filtering ssl block-server**.
- С помощью разрыва SSL между WEB-сервером и клиентом и установления отдельного соединения с каждым из них. Для включения данного режима работы используется атрибут **set service webproxy url-filtering ssl bump-server**.

В качестве значения для данных атрибутов указываются домены, либо регулярные выражения описывающие один и более доменов. Работа этих способов возможна параллельно, в таком случае атрибут **block-server** является приоритетным.

Блокировка SSL по SNI

Данный метод осуществляет фильтрацию трафика без подмены сертификатов сайтов. На этапе установления SSL соединения клиента с WEB-сервером прокси сервер анализирует поле SNI (Server Name Indication,RFC 6066). Далее, принимается решение о разрешении или запрете дальнейшего соединения. Данный метод не позволяет использовать функционал из блока конфигурации squidguard, и ограничен только фильтрацией определенных доменов. Однако, этот метод не осуществляет MITM между клиентом и WEB-сервером и не требует добавления самоподписанного сертификата удостоверяющего центра в список доверенных сертификатов клиента.

Разрыв SSL соединения

При использовании метода с разрывом SSL соединения важным моментом является создание сертификата, который прокси-сервер будет предоставлять конечным пользователям. Так как от этого зависит, будут ли выдаваться предупреждения системы безопасности в браузерах конечных пользователей. Предупреждения могут выдаваться в следующих случаях:

- Предоставляемый прокси-сервером сертификат подписан УЦ, который не является доверенным для конечного пользователя.
- Имя, указанное в сертификате, не соответствует доменному имени сайта.
- Срок действия сертификата не соответствует установленному времени и дате на клиентском устройстве.

Поэтому, для того чтобы в браузерах клиентов не выдавались предупреждения безопасности должны быть произведены следующие настройки:

- Сертификат УЦ, указанный в настройках прокси-сервера, должен находиться в списке доверенных удостоверяющих центров для конечных пользователей.
- На клиентских устройствах и на Numa Edge должна быть настроена одинаковая время и дата. Для этих целей рекомендуется использовать службу синхронизации точного времени (NTP).

Генерация сертификатов WEB-серверов, к которым подключается клиент производится автоматически. Для этого прокси сервер "подсматривает" сообщение TLS ClientHello и, на основе полученного значения поля SNI, в котором содержится доменное имя сайта, генерирует новый сертификат.

Прокси сервер также устанавливает SSL соединение и с реальным WEB-сервером, к которому обращается клиент. Поэтому на Numa Edge должны быть импортированы сертификаты УЦ, которым подписан сертификат этого WEB-сервера, для того чтобы полученный сертификат прошел проверку подлинности.

ПРИМЕЧАНИЕ В том случае если проверка сертификатов удаленных серверов отключена, будут приниматься все сертификаты, включая те, которые не прошли проверку. В связи с этим отключение проверки сертификатов удаленных серверов строго не рекомендуется, так как в этом случае нельзя гарантировать надежность серверов и безопасность устанавливаемых соединений.

25.3.4 Аутентификация пользователей прокси

Прокси-сервер для предоставления доступа к ресурсам сети может осуществлять аутентификацию и авторизацию пользователей. Возможно построение взаимодействия с сервером LDAP и аутентификации на основе регистрационного имени и пароля, а также с сервером Microsoft Active Directory и сквозной аутентификации клиентов — членов домена, используя протокол NTLM.

При использовании аутентификации и авторизации пользователей возможна работа только в непрозрачном режиме прокси, при этом на клиентском ПО должны быть соответствующим образом прописаны настройки прокси-сервера.

При использовании аутентификации на основе LDAP, пользователю выдается приглашение на ввод регистрационного имени и пароля.

Процесс аутентификации при использовании NTLM отличается в зависимости от используемого браузера. В том случае если пользователь является членом домена и использует веб-браузер с поддержкой NTLM, аутентификация является сквозной, то есть не требует участия пользователя. Приглашение на ввод имени пользователя и пароля выдается только в случае невозможности аутентификации на базе NTLM.

25.3.5 "Прозрачный" и "непрозрачный" режимы

"Прозрачный" режим не предполагает какой-либо дополнительной настройки ПО пользователей и при "обычной" работе с ресурсами Интернет присутствие посредника не выявляется. Обычно посредник ожидает соединения на сетевом порту с номером, отличным от 80-го, поэтому в таких конфигурациях на границе защищаемой при помощи посредника сети принимаются меры для принудительного перенаправления всего трафика TCP, адресованного на порт 80 (а также на другие используемые сетевые порты, например, 443), на порт, прослушиваемый прокси-сервером. Прозрачность также исключает явную аутентификацию пользователей прокси (например, на основе идентификатора пользователя и пароля), но позволяет ограничивать запросы, например, по IP-адресу источника.

В "непрозрачном" режиме в клиентском ПО необходимо явно прописывать IP-адрес интерфейса системы и номер порта TCP, на котором ожидает соединений от клиентов программа-посредник. Считается, что поддерживающее работу через прокси клиентское ПО лучше работает через него когда он в "непрозрачном" режиме, то есть когда ПО "знает" о его существовании и может соответственно подстроить своё поведение. Кроме того, не всё вредоносное ПО обращает внимание на настройки прокси и умеет работать через него. Тем не менее, для "веб" вирусов (написанных, например, на flash или javascript и работающих в браузере) сам по себе прокси обычно не является преградой.

В обоих режимах отсутствует "прямое" (в смысле TCP) соединение между клиентом и его адресатом в Интернет. Вместо него присутствуют два соединения - между клиентом и прокси и между прокси и адресатом клиента в Интернет. Отличие в данном контексте в том, что в "прозрачном" режиме прокси представляет клиенту всё так, как будто между клиентом и его адресатом установлено "прямое" соединение.

По умолчанию прокси в системе Numa Edge работает в "прозрачном" режиме.

ПРЕДУПРЕЖДЕНИЕ Для корректной работы webproxy в прозрачном режиме также необходимо вручную настроить NAT.

При использовании аутентификации пользователей необходимо отключить "прозрачный" режим, для этого используется команда `service webproxy listen-address _ipv4_адрес_ disable-transparent`.

При настройке прокси-сервера в прозрачном режиме в системе дополнительно резервируется порт, номер которого на единицу меньше, чем номер порта по умолчанию. По умолчанию установлен порт 3128, поэтому для прокси-сервера в прозрачном режиме будет также зарезервирован порт с номером 3127. Этот порт будет использован для прямого доступа к ресурсам прокси-сервера (например, элементам служебных страниц) при необходимости.

При настройке прокси-сервера в прозрачном режиме и включенном режиме проксирования SSL резервируется порт, номер которого на единицу больше номера порта по умолчанию (в данном случае номер порта с защищенным соединением будет равен 3129).

25.4 Команды настройки фильтрации веб-содержимого и управления веб-прокси

Команды, связанные с фильтрацией запросов	
service webproxy domain-block <домен>	Запрещает доступ к указанному домену.
service webproxy reply-block-mime <тип_mime>	Запрещает доступ к веб-содержимому указанного типа mime.
service webproxy url-filtering disable	Выключает фильтрацию без потери настроек.
service webproxy url-filtering squidguard allow-category <категория>	Разрешает доступ по адресам из указанной категории.
service webproxy url-filtering squidguard block-category <категория>	Запрещает доступ по адресам из указанной категории.
service webproxy url-filtering squidguard allow-ipaddr-url	Разрешает запросы, в URL которых указан IP-адрес, а не доменное имя.
service webproxy url-filtering squidguard default-action <действие>	Задаёт действие, которое будет применяться ко всем запросам, не попавшим под имеющиеся фильтры.
service webproxy url-filtering squidguard enable-safe-search	Включает режим безопасного поиска ("Safe Search") на популярных поисковых системах.
service webproxy url-filtering squidguard local-block <адрес>	Запрещает доступ к указанному адресу IP или домену.
service webproxy url-filtering squidguard local-block-keyword <ключ>	Блокирует запросы к URL, если в нем содержится указанное ключевое значение.
service webproxy url-filtering squidguard local-block-url <адрес>	Блокирует запросы к указанному URL.
service webproxy url-filtering squidguard local-ok <адрес>	Разрешает доступ к указанному адресу IP или домену.
service webproxy url-filtering squidguard local-ok-url <адрес>	Разрешает доступ по указанному URL.
service webproxy url-filtering squidguard log <категория>	Включает протоколирование в журнальном файле запросов пользователей по URL из указанной категории.
service webproxy url-filtering squidguard redirect-url <адрес>	При обращении к адресу из "чёрного" списка пользователю будет возвращено содержимое по указанному URL вместо запрошенного.
service webproxy url-filtering squidguard rule <номер>	Создаёт (пустое) правило фильтрации с указанным номером.

service webproxy url-filtering squidguard rule <номер> allow-category <категория>	Разрешает доступ к веб-содержимому по адресам из указанной категории в пределах правила.
service webproxy url-filtering squidguard rule <номер> block-category <категория>	Запрещает доступ к веб-содержимому по адресам из указанной категории в пределах правила.
service webproxy url-filtering squidguard rule <номер> allow-ipaddr-url	Разрешает запросы в указанном правиле, у которых в URL указан IP-адрес, а не доменное имя.
service webproxy url-filtering squidguard rule <номер> default-action <действие>	Задаёт действие по умолчанию для указанного правила.
service webproxy url-filtering squidguard rule <номер> description <описание>	Задаёт человеческое (словесное) описание указанного правила.
service webproxy url-filtering squidguard rule <номер> enable-safe-search	Включает режим безопасного поиска ("Safe Search") на популярных поисковых системах для указанного правила.
service webproxy url-filtering squidguard rule <номер> local-block <адрес>	Запрещает доступ к указанному адресу IP или URL в пределах правила.
service webproxy url-filtering squidguard rule <номер> local-block-file <маска>	Запрещает имена файлов согласно указанной маски , используя для поиска последний сегмент компонента Path URI запроса.
service webproxy url-filtering squidguard rule <номер> local-block-url <адрес>	Блокирует запросы к URL, если в нем содержится указанное ключевое значение в данном правиле.
service webproxy url-filtering squidguard rule <номер> local-block-keyword <ключ>	Блокирует в рамках правила запросы к содержимому, URL которого содержит указанный набор символов.
service webproxy url-filtering squidguard rule <номер> local-ok <адрес>	Разрешает доступ к указанному адресу IP или URL в пределах правила.
service webproxy url-filtering squidguard rule <номер> local-ok-file <маска>	Разрешает имена файлов согласно указанной маски , используя для поиска последний сегмент компонента Path URI запроса.
service webproxy url-filtering squidguard rule <номер> local-ok-url <адрес>	Разрешает доступ по указанному IP или URL в пределах правила.
service webproxy url-filtering squidguard rule <номер> log <категория>	Включает в пределах указанного правила протоколирование запросов пользователей к адресам из определенной категории.
service webproxy url-filtering squidguard rule <номер> metod-block <метод>	Указывает HTTP метод, при использовании которого запрос будет запрещен.
service webproxy url-filtering squidguard rule <номер> metod-ok <метод>	Указывает HTTP метод, при использовании которого запрос будет разрешен.
service webproxy url-filtering squidguard rule <номер> redirect-url <адрес>	Изменяет URL, содержимое которого возвращается вместо запрошенного при обращении к адресам из "чёрного" списка в указанном правиле.
service webproxy url-filtering squidguard rule <номер> source-group <имя_группы>	Задаёт группу пользователей, к которой будет применяться правило с указанным номером.
service webproxy url-filtering squidguard rule <номер> time-period <имя_промежутка>	Задаёт промежуток времени, в течение которого правило с указанным номером будет актуальным.
service webproxy url-filtering squidguard source-group <имя_группы>	Объявляет (пустую) группу пользователей.
service webproxy url-filtering squidguard source-group <имя_группы> address <адрес>	Добавляет указанные адрес или сеть IPv4 в члены группы с указанным именем.
service webproxy url-filtering squidguard source-group <имя_группы> description <описание>	Задаёт человеческое (словесное) описание указанной группы пользователей.

service webproxy url-filtering squidguard source-group <имя_группы> domain <домен>	Добавляет указанный домен в члены группы с указанным именем.
service webproxy url-filtering squidguard source-group <имя_группы> ldap-group <имя_LDAP_группы>	Добавление пользователей, относящихся к данной группе пользователей LDAP, в члены указанной группы.
service webproxy url-filtering squidguard source-group <имя_группы> user <имя_пользователя>	Добавляет пользователя, успешно прошедшего аутентификацию, в члены указанной группы.
service webproxy url-filtering squidguard time-period <имя_промежутка>	Объявляет промежуток времени, который можно потом использовать в правилах.
service webproxy url-filtering squidguard time-period <имя_промежутка> days <день> time <время>	Задаёт день (дни) и диапазон времени суток для указанного промежутка времени.
service webproxy url-filtering squidguard time-period <имя_периода> description <описание>	Задаёт человеческое (словесное) описание указанного промежутка времени.
Команды, связанные с настройкой журналирования событий webproxy	
service webproxy request-log logfile <режим>	Включение регистрации отчетов модуля веб-прокси в локальном файле регистрации.
service webproxy request-log syslog	Включение регистрации отчетов модуля веб-прокси в системном журнале.
service webproxy request-log syslog facility <источник>	Указание источника сообщений, от имени которого модуль веб-прокси будет отправлять сообщения в системный журнал.
service webproxy request-log syslog level <уровень>	Указание уровня серьезности сообщений модуля веб-прокси, которые будут регистрироваться в системном журнале.
service webproxy request-log sql-db db-name <имя>	Указание имени внешней базы данных для регистрации отчетов модуля веб-прокси.
service webproxy request-log sql-db db-type <имя>	Указание типа СУБД, используемой для регистрации отчетов системы веб-прокси.
service webproxy request-log sql-db host <адрес>	Указание адреса или символьного имени сервера БД для подключения.
service webproxy request-log sql-db username <имя_пользователя>	Указание имени пользователя, от имени которого будет осуществляться запись в БД.
service webproxy request-log sql-db password <пароль>	Указание пароля пользователя.
Команды, связанные с настройкой внешнего сервера ICAP	
service webproxy icap filter <режим>	Настройка режима фильтрации запросов/ответов.
service webproxy icap persistent-connections <режим>	Настройка режима постоянного соединения с сервером ICAP.
service webproxy icap preview <режим>	Настройка режима preview для сервера ICAP.
service webproxy icap send-client-ip <режим>	Настройка указания IP-адреса клиента в запросе ICAP.
service webproxy icap server-address <ipv4-адрес>	Указание IP-адреса сервера ICAP.
service webproxy icap server-port <порт>	Указание порта сервера ICAP.
service webproxy icap service-name <имя>	Указание имени сервера ICAP.
Команды, связанные с настройкой проксирования соединений SSL	
service webproxy listen-address <ipv4_адрес>	Включает режим проксирования соединений SSL

enable-ssl	
service webproxy ssl disable-verify	Отключить проверку сертификатов удаленных серверов при включенном проксировании соединений SSL.
service webproxy ssl x509-cert <имя_сертификата>	Указание сертификата удостоверяющего центра, который будет использоваться прокси-сервером для генерации подменных сертификатов.
service webproxy url-filtering ssl block-server [name <домен> | regex <выражение>]	Настройка блокировки домена, соединение с которым зашифровано с помощью SSL.
service webproxy url-filtering ssl bump-server [name <домен> | regex <выражение>]	Настройка перехвата SSL/TLS соединения между веб-сайтом и клиентом для последующей настройки фильтрации.
Команды управления кэшированием	
service webproxy cache-size <размер>	Задаёт объём хранилища для временного хранения содержимого (кэша).
service webproxy domain-noncache <домен>	Выключает кэширование данных, полученных с указанного домена.
service webproxy maximum-object-size <размер>	Прокси будет помещать в кэш объекты с размером не больше указанного.
service webproxy minimum-object-size <размер>	Прокси будет помещать в кэш только объекты с размером не меньше указанного.
Команды, связанные с аутентификацией пользователей	
service webproxy authentication method <метод>	Указание используемого метода аутентификации пользователей прокси.
service webproxy authentication ntlm name <имя>	Указание имени компьютера в домене.
service webproxy authentication ntlm password <пароль>	Указание пароля для учётной записи пользователя, которая используется для авторизации в домене.
service webproxy authentication ntlm pdc <адрес>	Указание IP-адреса или имени контроллера домена.
service webproxy authentication ntlm user <имя_пользователя>	Указание имени пользователя для авторизации в домене.
service webproxy authentication ntlm workgroup <имя_домена>	Указание имени домена.
service webproxy authentication radius address <адрес>	Указание IP-адреса сервера RADIUS для аутентификации в веб-прокси.
service webproxy authentication radius port <порт>	Указание порта сервера RADIUS для аутентификации в веб-прокси.
service webproxy authentication radius digest-type <алгоритм>	Указание алгоритма хеширования для протокола RADIUS для аутентификации в веб-прокси.
service webproxy authentication radius secret <ключ>	Указание разделяемого ключа для аутентификации в веб-прокси через сервер RADIUS.
Команды управления самим сервером веб-прокси и просмотра его состояния	
service webproxy append-domain <домен>	Указанное доменное имя будет присоединяться к URL, не содержащим точек.
service webproxy access-ports [http <порт> | https <порт>]	Задание списка разрешенных портов назначения, с которыми может устанавливать соединение клиент, используя заданный протокол.
service webproxy forwarded-for <режим>	Настройка X-Forwarded-For заголовка.

service webproxy host-verify-policy <тип_верификации>	Настройка действия в случае ошибки верификации заголовка «Host» в режиме прозрачного прокси.
service webproxy identity admin-email <адрес>	Задаёт адрес электронного почтового ящика администратора веб-прокси
service webproxy identity hostname <имя>	Задаёт имя системы, которым веб-прокси будет обозначать себя.
service webproxy listen-address <ipv4_адрес>	Задаёт IPv4-адрес сетевого интерфейса, на котором веб-прокси будет ожидать соединений.
service webproxy listen-address <ipv4_адрес> disable-transparent	Выключает "прозрачный" режим работы для соединений, поступающих на интерфейс с указанным адресом.
service webproxy listen-address <ipv4-адрес> http-port <порт>	Изменяет порт, на котором веб-прокси ожидает HTTP трафик.
service webproxy listen-address <ipv4_адрес> https-port <порт>	Изменяет порт, на котором веб-прокси ожидает HTTPS трафик.
service webproxy restart	Перезапускает процесс веб-прокси.
service webproxy show blacklist categories	Показывает перечень категорий, доступ к которым закрыт ("чёрный" список категорий).
service show webproxy blacklist domains	Показывает перечень доменов, доступ к которым закрыт ("чёрный" список доменов).
service webproxy show blacklist log	Выводит протокол (журнал) запросов по адресам, находящимся в "чёрных" списках.
service webproxy show blacklist search <текст>	Ищет в "чёрных" списках домены и/или адреса, включающие в себя указанный текст.
service webproxy show blacklist urls	Показывает перечень адресов (URL), доступ к которым закрыт ("чёрный" список URL).
service webproxy show log	Вывод на экран протокола (журнала) всех запросов пользователей к веб-прокси.

25.4.1 service webproxy domain-block <домен>

Запрещает доступ к указанному домену.

Синтаксис

```
set service webproxy domain-block <домен>
delete service webproxy domain-block <домен>
show service webproxy domain-block
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        domain-block домен
    }
}
```

Параметры

домен

Множественный узел. Домен, доступ к которому нужно закрыть.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для запрета доступа к отдельному домену. Например, указание “facebook.com” в качестве аргумента закроет весь доступ к домену facebook.com и его поддоменам, а указание “.cn” закроет доступ ко всем сайтам доменной зоны Китая.

Форма **set** этой команды используется для задания нового домена, к которому нужно закрыть доступ.

Форма **delete** этой команды используется для восстановления доступа к указанному домену.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.2 service webproxy reply-block-mime <тип_mime>

Запрещает доступ к веб-содержимому указанного типа mime.

Синтаксис

```
set service webproxy reply-block-mime <тип_mime>
delete service webproxy reply-block-mime
show service webproxy reply-block-mime
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      reply-block-mime тип_mime {
      }
   }
}
```

Параметры

тип_mime

Тип mime, доступ к которому будет закрыт. Типы mime задаются в виде “тип/подтип”. К примеру, тип mime видео в формате Quicktime выглядит как “video/quicktime”, тип mime для файлов в формате PDF - как “application/pdf”, а тип mime для файлов .wav - как “audio/wav”.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для управления доступом к содержимому с указанным типом mime.

Форма **set** команды используется для закрытия доступа к данным с указанным типом mime.

Форма **delete** предназначена для восстановления доступа к данным с указанным типом mime.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.3 service webproxy url-filtering disable

Отключает фильтрацию веб-содержимого без потери/стирания конфигурации.

Синтаксис

```
set service webproxy url-filtering disable
delete service webproxy url-filtering disable
```

```
show service webproxy url-filtering
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            disable
        }
    }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для включения/отключения фильтрации запросов пользователей без потери конфигурации.

Форма **set** команды используется для выключения фильтрации.

Форма **delete** команды используется для включения фильтрации.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.4 service webproxy url-filtering squidguard allow-category <категория>

Разрешает доступ по URL из указанной категории.

Синтаксис

```
set service webproxy url-filtering squidguard allow-category <категория>
delete service webproxy url-filtering squidguard allow-category <категория>
show service webproxy url-filtering squidguard allow-category
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            squidguard {
                allow-category категория
            }
        }
    }
}
```

Параметры

категория

Множественный узел. Название категории, доступ по URL из которой нужно открыть, либо ключевое слово **all** для разрешения доступа по URL всех категорий.

Значение по умолчанию

Разрешает доступ по URL всех категорий.

Указания по использованию

Эта команда предназначена для разрешения доступа по URL, составляющим одну или несколько категорий. Наборы доступных категорий на разных устройствах могут отличаться.

Форма **set** команды используется для разрешения доступа по URL из указанной категории.

Форма **delete** команды используется для закрытия доступа по URL из указанной категории.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.5 service webproxy url-filtering squidguard block-category <категория>

Запрещает доступ по адресам из указанной категории.

Синтаксис

```
set service webproxy url-filtering squidguard block-category <категория>
delete service webproxy url-filtering squidguard block-category <категория>
show service webproxy url-filtering squidguard block-category
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      url-filtering {
         squidguard {
            block-category категория
         }
      }
   }
}
```

Параметры

категория

Множественный узел. Название категории, доступ по всем адресам (URL) из которой нужно закрыть, либо ключевое слово **all** для закрытия доступа по URL всех категорий.

Значение по умолчанию

Запрещает доступ по адресам (URL) всех категорий.

Указания по использованию

Эта команда предназначена для закрытия доступа по URL, составляющим одну или несколько категорий.

Наборы доступных на разных устройствах категорий могут отличаться..

Форма **set** команды используется для закрытия доступа по всем URL из указанной категории.

Форма **delete** команды используется для разрешения доступа по всем URL из указанной категории.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.6 service webproxy url-filtering squidguard allow-ipaddr-url

Разрешает запросы, в URL которых указан IP-адрес, а не доменное имя.

Синтаксис

```
set service webproxy url-filtering squidguard allow-ipaddr-url
delete service webproxy url-filtering squidguard allow-ipaddr-url
show service webproxy url-filtering squidguard
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            squidguard {
                allow-ipaddr-url
            }
        }
    }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Запросы по URL, содержащим адреса IP вместо доменных имён, блокируются.

Указания по использованию

По умолчанию, обращения по URL с адресами IP вместо доменных имён (вроде "http://123.234.34.56/some/path") блокируются. Эта команда предназначена для разрешения доступа по URL с адресами IP вместо доменных имён.

Форма **set** команды используется для разрешения доступа по URL с адресами IP вместо доменных имён.

Форма **delete** команды используется для восстановления поведения по умолчанию, запрещающего такой доступ.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.7 service webproxy url-filtering squidguard default-action <действие>

Задаёт действие, которое будет применяться ко всем запросам, не попавшим под имеющиеся фильтры.

Синтаксис

```
set service webproxy url-filtering squidguard default-action <действие>
delete service webproxy url-filtering squidguard default-action
show service webproxy url-filtering squidguard default-action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            squidguard {
                default-action действие
```

```
            }
        }
    }
}
```

Параметры

действие

Определяет реакцию посредника на запросы, не попавшие под имеющиеся у него фильтры. Допустимые значения:

allow: пропускать такие запросы;

block: блокировать такие запросы.

Значение по умолчанию

Запросы, не попавшие под имеющиеся у веб-прокси фильтры, пропускаются (**allow**).

Указания по использованию

Эта команда предназначена для изменения реакции веб-прокси на запросы, не попавшие под имеющиеся у него фильтры.

Форма **set** команды используется для изменения реакции на указанную в параметре.

Форма **delete** команды используется для восстановления поведения по умолчанию ("запросы, не попавшие под фильтры, пропускаются")

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.8 service webproxy url-filtering squidguard enable-safe-search

Включает режим безопасного поиска ("Safe Search") на популярных поисковых системах.

Синтаксис

```
set service webproxy url-filtering squidguard enable-safe-search
delete service webproxy url-filtering squidguard enable-safe-search
show service webproxy url-filtering squidguard
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            squidguard {
                enable-safe-search
            }
        }
    }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Режим безопасного поиска выключен.

Указания по использованию

Эта команда включает такое изменение запросов к популярным поисковым системам, при котором они исключают из результатов поиска нежелательные (по принятым у них критериям) результаты. В настоящее время поддерживаются следующие поисковые системы: Google, Yahoo и Bing.

Форма **set** команды используется для включения режима безопасного поиска на поддерживаемых поисковых системах.

Форма **delete** команды используется для выключения режима безопасного поиска на поддерживаемых поисковых системах.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.9 service webproxy url-filtering squidguard local-block <адрес>

Запрещает доступ к указанному адресу IP или домену.

Синтаксис

```
set service webproxy url-filtering squidguard local-block <адрес>
delete service webproxy url-filtering squidguard local-block <адрес>
show service webproxy url-filtering squidguard local-block
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      url-filtering {
         squidguard {
            local-block адрес
         }
      }
   }
}
```

Параметры

адрес

Множественный узел. Адрес IP или домен, доступ к которым надо запретить. Вводить значение нужно без «http://».

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для запрета доступа к отдельным адресам IP и/или доменам, которые могут и не принадлежать поддерживаемым прокси категориям адресов.

Форма **set** команды используется для закрытия доступа к указанному адресу IP или домену.

Форма **delete** команды используется для восстановления доступа к указанному адресу IP или домену, если ранее он был закрыт.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.10 service webproxy url-filtering squidguard local-block-keyword <ключ>

Блокирует запросы к содержимому, URL которого содержит указанный в качестве ключа набор символов.

Синтаксис

```
set service webproxy url-filtering squidguard local-block-keyword <ключ>
delete service webproxy url-filtering squidguard local-block-keyword <ключ>
show service webproxy url-filtering squidguard local-block-keyword
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            squidguard {
                local-block-keyword ключ
            }
        }
    }
}
```

Параметры

ключ

Множественный узел. Простая строка символов или регулярное выражение, совпадение которых с чем-либо в URL вызовет блокировку содержащего этот URL запроса.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда позволяет задавать строки и/или регулярные выражения, присутствие которых или совпадения с которыми чего-либо в URL запросах вызовет блокировку этих запросов. Благодаря этому можно управлять доступом к содержимому и сайтам, не относящимся к известным веб-прокси категориям.

ПРИМЕЧАНИЕ Следует уделять большое внимание указываемым строкам и регулярным выражениям, так как что-то слишком общее или просто неправильное может закрыть доступ и к тем ресурсам, которые должны быть доступны. Кроме того, такие проверки (поиск вхождения строк и применение регулярных выражений) требуют много вычислительных ресурсов и могут сильно снизить производительность устройства в целом.

Форма **set** команды используется для задания строки или регулярного выражения, присутствие которой или совпадение с которым будет проверяться для URL из каждого запроса.

Форма **delete** команды используется для исключения из участия в проверках указанной строки или регулярного выражения.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.11 service webproxy url-filtering squidguard local-block-url <адрес>

Блокирует запросы к содержимому, URL которого совпадает с указанным.

Синтаксис

```
set service webproxy url-filtering squidguard local-block-url <адрес>
delete service webproxy url-filtering squidguard local-block-url <адрес>
show service webproxy url-filtering squidguard local-block-url
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      url-filtering {
         squidguard {
            local-block-url адрес
         }
      }
   }
}
```

Параметры

адрес

Множественный узел. URL, доступ к которому нужно закрыть. Вводить значение нужно без «http://».

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для запрета доступа по указанному в ней URL. В ней можно указывать любые адреса, в том числе и не имеющие отношения к известным веб-прокси категориям.

Форма **set** команды используется для закрытия доступа по указанному в ней URL.

Форма **delete** команды используется для восстановления доступа по указанному в ней URL, если ранее он был закрыт.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.12 service webproxy url-filtering squidguard local-ok <адрес>

Разрешает доступ к указанному адресу IP или домену.

Синтаксис

```
set service webproxy url-filtering squidguard local-ok <адрес>
delete service webproxy url-filtering squidguard local-ok <адрес>
show service webproxy url-filtering squidguard local-ok
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      url-filtering {
         squidguard {
            local-ok адрес
         }
      }
   }
}
```

Параметры

адрес

Множественный узел. Адрес IP или домен, доступ к которому нужно разрешить. Вводить значение нужно без «http://».

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для явного разрешения доступа к отдельным IP-адресам и/или доменам, которые могут быть заблокированы какими-то общими правилами или, например, в рамках категорий.

Форма **set** команды используется для явного разрешения доступа по указанному в ней адресу IP или домену.

Форма **delete** команды используется для отмены явного разрешения доступа к указанному в ней адресу IP или домену.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.13 service webproxy url-filtering squidguard local-ok-url <адрес>

Разрешает доступ по указанному URL.

Синтаксис

```
set service webproxy url-filtering squidguard local-ok-url <адрес>
delete service webproxy url-filtering squidguard local-ok-url <адрес>
show service webproxy url-filtering squidguard local-ok-url
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      url-filtering {
         squidguard {
            local-ok-url адрес
         }
      }
   }
}
```

Параметры

адрес

Множественный узел. URL, доступ к которому нужно разрешить. Вводить значение нужно без «http://».

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для явного разрешения доступа к указанному в ней URL, который может быть заблокирован каким-то общим правилом или например, в рамках категорий.

Форма **set** команды используется для явного разрешения доступа по указанному в ней URL.

Форма **delete** команды используется для отмены явного разрешения доступа к указанному в ней URL.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.14 service webproxy url-filtering squidguard log <категория>

Включает протоколирование в журнальном файле запросов пользователей по URL из указанной категории.

Синтаксис

```
set service webproxy url-filtering squidguard log <категория>
delete service webproxy url-filtering squidguard log <категория>
show service webproxy url-filtering squidguard log
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      url-filtering {
         squidguard {
            log категория
         }
      }
   }
}
```

Параметры

категория

Множественный узел. Название категории, информацию о запросах пользователей по URL из которой нужно сохранять в файлах-журналах. Для включения протоколирования по всем категориям сразу можно использовать ключевое слово **all**.

Значение по умолчанию

Факты обращения по URL из известных веб-прокси категорий в файлы-журналы не заносятся.

Указания по использованию

Эта команда предназначена для включения записи в журнал доступа информации о фактах обращения пользователей по URL, перечисленным в указанной в команде категории (либо во всех категориях, если указано ключевое слово **all**).

Форма **set** команды используется для включения протоколирования обращений по URL из указанной категории (или из всех, если указано ключевое слово **all**).

Форма **delete** команды используется для выключения протоколирования обращений по URL из указанной категории (или из всех, если указано ключевое слово **all**).

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.15 service webproxy url-filtering squidguard redirect-url <адрес>

При обращении к адресу из "чёрного" списка возвращать пользователю содержимое по указанному URL вместо запрошенного.

Синтаксис

```
set service webproxy url-filtering squidguard redirect-url <адрес>
delete service webproxy url-filtering squidguard redirect-url
show service webproxy url-filtering squidguard redirect-url
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            squidguard {
                redirect-url адрес
            }
        }
    }
}
```

Параметры

адрес

Содержимое, доступное по этому URL, будет возвращено в ответ на запросы пользователей по URL из "чёрного" списка.

Значение по умолчанию

При попытке обращения по адресу из "чёрного" списка пользователю будет возвращено содержимое по предопределённому адресу.

Указания по использованию

Эта команда задаёт URL, содержимое по которому будет возвращено в ответ на запросы пользователей по адресам из "чёрного" списка.

ПРИМЕЧАНИЕ Важно убедиться в том, что доступ к содержимому этой URL не закрыт каким-либо правилом. Например, если действием по умолчанию для всех запросов является запрет доступа и доступ по этому URL не разрешён явно каким-то правилом (скажем, через **local-ok**), то пользователи в ответ на свои запросы по адресам из "чёрного" списка будут получать страницу с сообщением о закрытом доступе по этому URL, что, возможно, не совсем то, что ожидалось.

Форма **set** команды используется для задания URL, содержимое по которому будет возвращено в ответ на обращение по адресу из "чёрного" списка.|

Форма **delete** команды используется для восстановления возврата содержимого по предопределённому адресу.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.16 service webproxy url-filtering squidguard rule <номер>

Создаёт (пустое) правило фильтрации с указанным номером.

Синтаксис

```
set service webproxy url-filtering squidguard rule <номер>
delete service webproxy url-filtering squidguard rule <номер>
show service webproxy url-filtering squidguard rule <номер>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            squidguard {
```

```
            rule номер {
            }
        }
    }
}
```

Параметры

номер

Множественный узел. Уникальный номер правила, в диапазоне он 1 до 1024.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для создания пустых правил фильтрации ("контейнеров").

Форма **set** команды используется для создания пустого правила фильтрации с указанным номером.

Форма **delete** используется для уничтожения правила фильтрации с указанным номером.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.17 service webproxy url-filtering squidguard rule <номер> allow-category <категория>

Разрешает доступ к веб-содержимому по адресам из указанной категории в рамках существующего правила.

Синтаксис

```
set service webproxy url-filtering squidguard rule <номер> allow-category <категория>
delete service webproxy url-filtering squidguard rule <номер> allow-category <категория>
show service webproxy url-filtering squidguard rule <номер> allow-category
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            squidguard {
                rule номер {
                    allow-category категория
                }
            }
        }
    }
}
```

Параметры

номер

Множественный узел. Номер правила.

категория

Множественный узел. Название категории, доступ по URL которой нужно разрешить, либо ключевое слово **all** для предоставления доступа по URL всех категорий.

Значение по умолчанию

Если категория не указана вообще, то разрешается доступ по URL из всех категорий.

Указания по использованию

Эта команда предназначена для внесения разрешения доступа по URL из указанной категории в указанное правило. Открыть доступ по URL из всех категорий сразу можно при помощи ключевого слова **all** в качестве названия категории.

Наборы доступных на разных устройствах категорий могут отличаться..

Форма **set** используется для разрешения доступа по URL из указанной категории в рамках указанного правила.

Форма **delete** используется для удаления разрешенной категории из правила фильтрации.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.18 service webproxy url-filtering squidguard rule <номер> block-category <категория>

Запрещает доступ к веб-содержимому по адресам из указанной категории в рамках существующего правила с указанным номером, либо создаёт новое правило с указанным номером и с таким запретом.

Синтаксис

```
set service webproxy url-filtering squidguard rule <номер> block-category <категория>
```

```
delete service webproxy url-filtering squidguard rule <номер> block-category <категория>
```

```
show service webproxy url-filtering squidguard rule <номер> block-category
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            squidguard {
                rule номер {
                    block-category категория
                }
            }
        }
    }
}
```

Параметры

номер

Множественный узел. Номер правила.

категория

Множественный узел. Название категории, доступ по URL которой нужно закрыть, либо ключевое слово **all** для закрытия доступа по URL всех категорий.

Значение по умолчанию

Если категория не указана вообще, то закрывается доступ по URL из всех категорий.

Указания по использованию

Эта команда предназначена для внесения запрета на доступ по URL из указанной категории в существующее правило либо для создания нового правила с таким запретом. Закрыть доступ по URL из всех категорий сразу можно при помощи ключевого слова **all** в качестве названия категории.

Наборы доступных на разных устройствах категорий могут отличаться. Ознакомиться с перечнем категорий, доступных на конкретном устройстве, можно при помощи команды .

Форма **set** используется для закрытия доступа по URL из указанной категории в рамках указанного правила, либо создаёт новое правило с указанным номером и таким запретом.

Форма **delete** используется для разрешения доступа по URL из указанной категории в рамках указанного существующего правила.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.19 service webproxy url-filtering squidguard rule <номер> allow-ipaddr-url

Разрешает запросы, в URL которых указан IP-адрес, а не доменное имя в указанном правиле.

Синтаксис

```
set service webproxy url-filtering squidguard rule <номер> allow-ipaddr-url
delete service webproxy url-filtering squidguard rule <номер> allow-ipaddr-url
show service webproxy url-filtering squidguard rule <номер>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            squidguard {
                rule номер {
                    allow-ipaddr-url
                }
            }
        }
    }
}
```

Параметры

номер

Множественный узел. Номер правила.

Значение по умолчанию

Запросы по URL, содержащим адреса IP вместо доменных имён, блокируются.

Указания по использованию

По умолчанию, обращения по URL с адресами IP вместо доменных имён (вроде "http://123.234.34.56/some/path") блокируются. Эту команду можно использовать для разрешения обращения по IP-адресам в рамках конкретного правила.

Форма **set** команды используется для разрешения доступа по URL с адресами IP вместо доменных имён в рамках конкретного правила.

Форма **delete** используется для восстановления поведения по умолчанию, запрещающего такой доступ в рамках конкретного правила.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.20 service webproxy url-filtering squidguard rule <номер> default-action <действие>

Установка действия по умолчанию, то есть которое будет применяться ко всем запросам, не попавшим под имеющиеся у веб-прокси фильтры.

Синтаксис

```
set service webproxy url-filtering squidguard rule <номер> default-action <действие>
delete service webproxy url-filtering squidguard rule <номер> default-action
show service webproxy url-filtering squidguard rule <номер> default-action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            squidguard {
                rule номер {
                    default-action действие
                }
            }
        }
    }
}
```

Параметры

номер

Множественный узел. Номер правила.

действие

Определяет реакцию посредника на запросы, не попавшие под имеющиеся у него фильтры. Допустимые значения:

allow: пропускать такие запросы;

block: блокировать такие запросы.

Значение по умолчанию

Запросы, не попавшие под имеющиеся у веб-прокси фильтры, пропускаются.

Указания по использованию

Эта команда предназначена для изменения реакции веб-прокси на запросы, не попавшие под имеющиеся у него фильтры. Реакция изменится на указанную в случае успешного применения правила с указанным номером.

Форма **set** команды используется для изменения реакции на указанную в параметре.

Форма **delete** команды используется для восстановления поведения по умолчанию ("запросы, не попавшие под фильтры, пропускаются").

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.21 service webproxy url-filtering squidguard rule <номер> description <описание>

Задаёт текстовое описание правила с указанным номером.

Синтаксис

```
set service webproxy url-filtering squidguard rule <номер> description <описание>
delete service webproxy url-filtering squidguard rule <номер> description
show service webproxy url-filtering squidguard rule <номер> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      url-filtering {
         squidguard {
            rule номер {
               description описание
            }
         }
      }
   }
}
```

Параметры

номер

Множественный узел. Номер правила.

описание

Краткое текстовое описание работы всего правила. Если описание содержит пробелы, то оно должно быть заключено в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

С помощью этой команды можно связать с указанным по номеру правилом текстовую информацию, помогающую понять его работу/предназначение. Текст будет добавлен к существующему правилу, либо будет создано новое правило с указанными номером и описанием.

Форма **set** команды используется для добавления описания к правилу с указанным номером, либо создания нового правила с указанными номером и описанием.

Форма **delete** команды используется для исключения описания из правила с указанным номером

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.22 service webproxy url-filtering squidguard rule <номер> enable-safe-search

Включает режим безопасного поиска ("Safe Search") на популярных поисковых системах для указанного правила.

Синтаксис

```
set service webproxy url-filtering squidguard rule <номер> enable-safe-search

delete service webproxy url-filtering squidguard rule <номер> enable-safe-search

show service webproxy url-filtering squidguard rule <номер>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      url-filtering {
         squidguard {
            rule номер {
               enable-safe-search
            }
         }
      }
   }
}
```

Параметры

номер

Множественный узел. Номер правила.

Значение по умолчанию

Режим безопасного поиска выключен.

Указания по использованию

Эта команда включает такое изменение запросов к популярным поисковым системам, при котором они исключают из результатов поиска нежелательные (по принятым у них критериям) результаты. В настоящее время поддерживаются следующие поисковые системы: Google, Yahoo и Bing.

Форма **set** команды используется для включения режима безопасного поиска на поддерживаемых поисковых системах.

Форма **delete** команды используется для выключения режима безопасного поиска на поддерживаемых поисковых системах.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.23 service webproxy url-filtering squidguard rule <номер> local-block <адрес>

Запрещает доступ к указанному адресу IP или по указанному URL в пределах правила с указанным номером.

Синтаксис

```
set service webproxy url-filtering squidguard rule <номер> local-block <адрес>

delete service webproxy url-filtering squidguard rule <номер> local-block <адрес>
```

```
show service webproxy url-filtering squidguard rule <номер> local-block
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      url-filtering {
         squidguard {
            rule номер {
               local-block адрес
            }
         }
      }
   }
}
```

Параметры

номер

Множественный узел. Номер правила.

адрес

Множественный узел. Адрес IP или URL, доступ к которым нужно закрыть.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для запрета доступа к отдельным адресам IP и/или доменам в рамках правила с указанным номером. Адрес или URL могут и не принадлежать к известным прокси адресам из поддерживаемых категорий.

Форма **set** команды используется для закрытия доступа к указанному адресу IP или домену.

Форма **delete** команды используется для восстановления доступа к указанному адресу IP или домену если ранее он был закрыт.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.24 service webproxy url-filtering squidguard rule <номер> local-block-file <маска>

Запрещает имена файлов согласно указанной маски , используя для поиска последний сегмент компонента Path URI запроса.

Синтаксис

```
set service webproxy url-filtering squidguard rule <номер> local-block-file
<маска>

delete service webproxy url-filtering squidguard rule <номер> local-block-
file <маска>

show service webproxy url-filtering squidguard rule <номер> local-block-file
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      url-filtering {
         squidguard {
            rule <номер> {
               local-block-file маска
            }
         }
      }
   }
}
```

Параметры

маска

Множественный узел. Задает маску имени файла в URI, доступ к которому будет заблокирован.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать имена файлов, доступ к которым будет заблокирован.

Доступны следующие значения:

- текстовое описание относительного имени файла или каталога;
- [] – описывается диапазон символов для сопоставления одного символа в этом диапазоне;
- ? – не в скобках соответствует одиночному символу;
- * – не в скобках соответствует любому количеству символов, в том числе и их отсутствию;
- ! – если указывается в скобках первым символом, то соответствует отрицанию данного диапазона;
- \ – экранирование, используется в скобках для сопоставления со спецсимволами.

Пример применения данного атрибута в правиле 10 для блокировки скачивания файлов с расширением *.exe : **set service webproxy url-filtering squidguard rule 10 local-block-file "*.exe"**

ПРИМЕЧАНИЕ Необходимо иметь в виду, что поскольку все веб-страницы так или иначе являются файлами, то данный метод подходит для фильтрации отдельных веб-страниц, поисковых запросов и элементов сайта (JS,CSS, HTML).

Форма **set** команды используется для задания маски, по которой будет производиться поиск в последнем сегменте компонента Path URI запроса. В случае совпадения запрос по данному URI будет заблокирован.
Форма **delete** команды используется для удаления ранее заданной маски.
Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.25 service webproxy url-filtering squidguard rule <номер> local-block-url <адрес>

Блокирует запросы к содержимому, URL которого совпадает с указанным.

Синтаксис

```
set service webproxy url-filtering squidguard rule <номер> local-block-url
<адрес>

delete service webproxy url-filtering squidguard rule <номер> local-block-url
<адрес>
```

```
show service webproxy url-filtering squidguard rule <номер> local-block-url
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            squidguard {
                rule <номер> {
                    local-block-url адрес
                }
            }
        }
    }
}
```

Параметры

адрес

Множественный узел. URL, доступ к которому нужно закрыть. Вводить значение нужно без «http://»..

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для запрета доступа по указанному в ней URL. В ней можно указывать любые адреса, в том числе и не имеющие отношения к известным веб-прокси категориям.

Форма **set** команды используется для закрытия доступа по указанному в ней URL.

Форма **delete** команды используется для восстановления доступа по указанному в ней URL, если ранее он был закрыт.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.26 service webproxy url-filtering squidguard rule <номер> local-block-keyword <ключ>

Блокирует в рамках правила с указанным номер запросы к содержимому, URL которого содержит указанный набор символов.

Синтаксис

```
set service webproxy url-filtering squidguard rule <номер> local-block-keyword <ключ>

delete service webproxy url-filtering squidguard rule <номер> local-block-keyword <ключ>

show service webproxy url-filtering squidguard rule <номер> local-block-keyword
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
```

```
            squidguard {
               rule номер {
                  local-block-keyword ключ
               }
            }
         }
      }
   }
```

Параметры

номер

Множественный узел. Номер правила.

ключ

Множественный узел. Простая строка символов или регулярное выражение, совпадение которых с чем-либо в URL вызовет блокировку содержащего этот URL запроса.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда позволяет задавать строки и/или регулярные выражения, присутствие которых или совпадения с которыми в URL запросов вызовет блокировку этих запросов. Благодаря этому можно управлять доступом к содержимому и сайтам, не относящимся к известным веб-прокси категориям.

ПРИМЕЧАНИЕ Следует уделять большое внимание указываемым строкам и регулярным выражениями, так как что-то слишком общее или просто неправильное может закрыть доступ и к тем ресурсам, которые должны быть доступны. Кроме того, такие проверки (поиск вхождения строк и применение регулярных выражений) требуют много вычислительных ресурсов и могут сильно снизить производительность устройства в целом.

Форма **set** команды используется для задания строки или регулярного выражения, присутствие которой или совпадение с которым будет проверяться для URL из каждого запроса.

Форма **delete** команды используется для исключения из участия в проверках указанные строку или регулярное выражение.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.27 service webproxy url-filtering squidguard rule <номер> local-ok <адрес>

Разрешает доступ к указанному адресу IP или URL в пределах правила.

Синтаксис

```
set service webproxy url-filtering squidguard rule <номер> local-ok <адрес>
delete service webproxy url-filtering squidguard rule <номер> local-ok <адрес>
show service webproxy url-filtering squidguard rule <номер> local-ok
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      url-filtering {
```

```
            squidguard {
               rule номер {
                  local-ok адрес
               }
            }
         }
      }
   }
```

Параметры

номер

Множественный узел. Номер правила.

адрес

Множественный узел. Адрес IP или домен, доступ к которому нужно разрешить. Вводить значение нужно без «http://».

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для явного разрешения доступа к отдельным IP-адресам и/или доменам, которые могут быть заблокированы какими-то общими правилами или, например, в рамках категорий.

Форма **set** команды используется для явного разрешения доступа по указанному в ней адресу IP или домену.

Форма **delete** команды используется для устранения явного разрешения доступа к указанному в ней адресу IP или домену.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.28 service webproxy url-filtering squidguard rule <номер> local-ok-file <маска>

Разрешает имена файлов согласно указанной маски , используя для поиска последний сегмент компонента Path URI запроса.

Синтаксис

```
set service webproxy url-filtering squidguard rule <номер> local-ok-file <маска>
delete service webproxy url-filtering squidguard rule <номер> local-ok-file <маска>
show service webproxy url-filtering squidguard rule <номер> local-ok-file
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      url-filtering {
         squidguard {
            rule <номер> {
               local-ok-file маска
            }
```

```
            }
        }
    }
}
```

Параметры

маска

Множественный узел. Задает маску имени файла в URI, доступ к которому будет разрешен.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать имена файлов, доступ к которым будет разрешен.

Доступны следующие значения:

- текстовое описание относительного имени файла или каталога;
- [] – описывается диапазон символов для сопоставления одного символа в этом диапазоне;
- ? – не в скобках соответствует одиночному символу;
- * – не в скобках соответствует любому количеству символов, в том числе и их отсутствию;
- ! – если указывается в скобках первым символом, то соответствует отрицанию данного диапазона;
- \ – экранирование, используется в скобках для сопоставления со спецсимволами.

Пример применения данного атрибута в правиле 10 для блокировки скачивания файлов с расширением *.css : **set service webproxy url-filtering squidguard rule 10 local-ok-file "*.css"**

ПРИМЕЧАНИЕ Необходимо иметь в виду, что поскольку все веб-страницы так или иначе являются файлами, то данный метод подходит для фильтрации отдельных веб-страниц, поисковых запросов и элементов сайта (JS,CSS, HTML).

Форма **set** команды используется для задания маски, по которой будет производиться поиск в последнем сегменте компонента Path URI запроса. В случае совпадения запрос по данному URI будет разрешен.
Форма **delete** команды используется для удаления ранее заданной маски.
Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.29 service webproxy url-filtering squidguard rule <номер> local-ok-url <адрес>

Разрешает доступ к указанному адресу IP или URL в пределах правила.

Синтаксис

```
set service webproxy url-filtering squidguard rule <номер> local-ok-url <адрес>
delete service webproxy url-filtering squidguard rule <номер> local-ok-url <адрес>
show service webproxy url-filtering squidguard rule <номер> local-ok-url
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            squidguard {
```

```
            rule <номер> {
                local-ok-url адрес
            }
        }
    }
}
```

Параметры

адрес

Множественный узел. URL, доступ к которому нужно разрешить. Вводить значение нужно без «http://».

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для явного разрешения доступа к указанному в ней URL, который может быть заблокирован каким-то общим правилом или например, в рамках категорий.

Форма **set** команды используется для явного разрешения доступа по указанному в ней URL.

Форма **delete** команды используется для отмены явного разрешения доступа к указанному в ней URL.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.30 service webproxy url-filtering squidguard rule <номер> log <категория>

Включает протоколирование в журнальном файле запросов пользователей по URL из указанной категории в случае успешной сверки условий указанного правила.

Синтаксис

```
set service webproxy url-filtering squidguard rule <номер> log <категория>
delete service webproxy url-filtering squidguard rule <номер> log <категория>
show service webproxy url-filtering squidguard rule <номер> log
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            squidguard {
                rule номер {
                    log категория
                }
            }
        }
    }
}
```

Параметры

номер

Множественный узел. Номер правила.

категория

Множественный узел. Название категории, информацию о запросах пользователей по URL которой нужно сохранять в файлах-журналах. Для включения протоколирования по всем категориям сразу можно использовать ключевое слово **all**.

Значение по умолчанию

Факты обращения по URL из известных модулю веб-прокси категорий в файлы-журналы не заносятся.

Указания по использованию

Эта команда предназначена для включения записи в журнал доступа информации о фактах обращения пользователей по URL, перечисленным в указанной в команде категории (либо во всех категориях, если указано ключевое слово **all**).

Форма **set** команды используется для включения протоколирования обращений по URL из указанной категории (или из всех, если указано ключевое слово **all**).

Форма **delete** команды используется для выключения протоколирования обращений по URL из указанной категории (или из всех, если указано ключевое слово **all**).

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.31 service webproxy url-filtering squidguard rule <номер> metod-block <метод>

Указывает HTTP метод, при использовании которого запрос будет запрещен.

Синтаксис

```
set service webproxy url-filtering squidguard rule <номер> metod-block <метод>
delete service webproxy url-filtering squidguard rule <номер> metod-block <метод>
show service webproxy url-filtering squidguard rule <номер> metod-block
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            squidguard {
                rule номер {
                    metod-block метод
                }
            }
        }
    }
}
```

Параметры

номер

Множественный узел. Номер правила.

метод

Множественный узел. Название метода, при использовании которого в HTTP запросе, данный запрос будет заблокирован.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для задания HTTP метода, при использовании которого в запросе, данный запрос будет заблокирован. В качестве значения ожидается текстовая строка, нечувствительная к регистру.

Форма **set** команды используется для задания HTTP метода, при использовании которого в запросе, данный запрос будет заблокирован.

Форма **delete** команды используется для удаления блокируемого HTTP метода.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.32 service webproxy url-filtering squidguard rule <номер> metod-ok <метод>

Указывает HTTP метод, при использовании которого запрос будет разрешен.

Синтаксис

```
set service webproxy url-filtering squidguard rule <номер> metod-ok <метод>
delete service webproxy url-filtering squidguard rule <номер> metod-ok <метод>
show service webproxy url-filtering squidguard rule <номер> metod-ok
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            squidguard {
                rule номер {
                    metod-ok метод
                }
            }
        }
    }
}
```

Параметры

номер

Множественный узел. Номер правила.

метод

Множественный узел. Название метода, при использовании которого в HTTP запросе, данный запрос будет разрешен.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для задания HTTP метода, при использовании которого в запросе, данный запрос будет разрешен. В качестве значения ожидается текстовая строка, нечувствительная к регистру.

Форма **set** команды используется для задания HTTP метода, при использовании которого в запросе, данный запрос будет разрешен.

Форма **delete** команды используется для удаления разрешенного HTTP метода.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.33 service webproxy url-filtering squidguard rule <номер> redirect-url <адрес>

Успешное применение указанного правила изменит URL, содержимое по которому возвращается вместо запрошенного при обращении к адресам из "чёрного" списка, на указанный.

Синтаксис

```
set service webproxy url-filtering squidguard rule <номер> redirect-url
<адрес>

delete service webproxy url-filtering squidguard rule <номер> redirect-url

show service webproxy url-filtering squidguard rule <номер> redirect-url
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            squidguard {
                rule номер {
                    redirect-url адрес
                }
            }
        }
    }
}
```

Параметры

номер

Множественный узел. Номер правила.

адрес

Содержимое, доступное по этому URL, будет возвращено в ответ на запросы пользователей по URL из "чёрного" списка.

Значение по умолчанию

При попытке обращения по адресу из "чёрного" списка пользователю будет возвращено содержимое по URL, заданному глобально при помощи команды .

Указания по использованию

Эта команда задаёт URL, содержимое по которому будет возвращено в ответ на запросы пользователей по адресам из "чёрного" списка.

ПРИМЕЧАНИЕ Важно убедиться в том, что доступ к содержимому по этому URL не закрыт каким-либо правилом. Например, если действием по умолчанию для всех запросов является запрет доступа и доступ по этому URL не разрешён явно каким-то правилом (скажем, через **local-ok**), то пользователи в ответ на свои запросы по адресам из "чёрного" списка будут получать страницу с сообщением о закрытом доступе по этому URL, что, возможно, не совсем то, что ожидалось.

Форма **set** команды используется для задания URL, содержимое по которому будет возвращено в ответ на обращение по адресу из "чёрного" списка.

Форма **delete** команды используется для восстановления возврата содержимого по глобальному URL.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.34 service webproxy url-filtering squidguard rule <номер> source-group <имя_группы>

Задаёт группу пользователей, к запросам которых будет применяться правило с указанным номером.

Синтаксис

```
set service webproxy url-filtering squidguard rule <номер> source-group <имя_группы>
delete service webproxy url-filtering squidguard rule <номер> source-group
show service webproxy url-filtering squidguard rule <номер> source-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      url-filtering {
         squidguard {
            rule номер {
               source-group имя_группы
            }
         }
      }
   }
}
```

Параметры

номер

Множественный узел. Номер правила.

имя_группы

Обязательный параметр. Название группы, к запросам пользователей которой будет применяться правило.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда позволяет указывать группы пользователей, к запросам которых будет применяться всё правило. Название группы должно указываться обязательно, сама группа должна быть определена заранее при помощи команды .

Форма **set** команды используется для задания имени группы для привязки к правилу.

Форма **delete** команды используется для отмены применение правила к запросам пользователей из указанной в команде группе.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.35 service webproxy url-filtering squidguard rule <номер> time-period <имя_промежутка>

Задаёт промежуток времени, в течение которого будет применяться правило с указанным номером.

Синтаксис

```
set service webproxy url-filtering squidguard rule <номер> time-period <имя_промежутка>
delete service webproxy url-filtering squidguard rule <номер> time-period
show service webproxy url-filtering squidguard rule <номер> time-period
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            squidguard {
                rule номер {
                    time-period имя_промежутка
                }
            }
        }
    }
}
```

Параметры

номер

Множественный узел. Номер правила.

имя_промежутка

Название промежутка времени.

Значение по умолчанию

Правило применяется независимо от промежутков и моментов времени.

Указания по использованию

Эта команда предназначена для указания промежутка времени, в течение которого будет применяться правило. Промежуток времени должен быть определён заранее.

Форма **set** команды используется для связывания с правилом промежутка времени, в течение которого правило будет применяться.

Форма **delete** команды используется для отмены временных ограничений на применение правила, восстанавливая поведение по умолчанию.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.36 service webproxy url-filtering squidguard source-group <имя_группы>

Объявляет (пустую) группу пользователей с указанным именем.

Синтаксис

```
set service webproxy url-filtering squidguard source-group <имя_группы>
delete service webproxy url-filtering squidguard source-group <имя_группы>
show service webproxy url-filtering squidguard source-group <имя_группы>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      url-filtering {
         squidguard {
            source-group имя_группы {
            }
         }
      }
   }
}
```

Параметры

имя_группы

Множественный узел. Название группы.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда позволяет создать пустую группу пользователей (контейнер), в которую позднее можно включить адреса IP или подсети систем пользователей. Такая группировка источников запросов делает управление доступом более гибким.

Форма **set** команды используется для создания (пустой) группы с указанным именем.

Форма **delete** команды используется для уничтожения группы с указанным именем.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.37 service webproxy url-filtering squidguard source-group <имя_группы> address <адрес>

Добавляет указанные адрес или подсеть IPv4 в члены указанной группы.

Синтаксис

```
set service webproxy url-filtering squidguard source-group <имя_группы> address <адрес>

delete service webproxy url-filtering squidguard source-group <имя_группы> address <адрес>

show service webproxy url-filtering squidguard source-group <имя_группы> address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      url-filtering {
         squidguard {
            source-group имя_группы {
               address адрес
            }
```

```
            }
        }
    }
}
```

Параметры

имя_группы

Множественный узел. Название группы.

адрес

Множественный узел. Адрес IPv4 подсети или отдельной системы.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для включения IPv4-адреса подсети или отдельной системы в указанную группу пользователей.

Форма **set** команды используется для включения указанного адреса в указанную группу.

Форма **delete** команды используется для исключения указанного адреса из указанной группы.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.38 service webproxy url-filtering squidguard source-group <имя_группы> description <описание>

Задаёт текстовое описание указанной группы пользователей.

Синтаксис

```
set service webproxy url-filtering squidguard source-group <имя_группы> description <описание>

delete service webproxy url-filtering squidguard source-group <имя_группы> description

show service webproxy url-filtering squidguard source-group <имя_группы> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            squidguard {
                source-group имя_группы {
                    description описание
                }
            }
        }
    }
}
```

Параметры

имя_группы

Множественный узел. Название группы.

описание

Краткое текстовое описание работы всего правила. Если описание содержит пробелы, то оно должно быть заключено в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

С помощью этой команды можно связать с указанной группой текстовую информацию, помогающую понять её предназначение.

Форма **set** команды используется для связывания указанного текстового описания с указанной группой.

Форма **delete** команды используется для исключения описания из указанной группу.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.39 service webproxy url-filtering squidguard source-group <имя_группы> domain <домен>

Добавляет системы пользователей, относящиеся к указанному домену, в члены указанной группы. IP-адреса систем или подсетей пользователей должны успешно разрешаться по обратной зоне DNS в указанное доменное имя.

Синтаксис

```
set service webproxy url-filtering squidguard source-group <имя_группы> domain <домен>
```

```
delete service webproxy url-filtering squidguard source-group <имя_группы> domain <домен>
```

```
show service webproxy url-filtering squidguard source-group <имя_группы> domain
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            squidguard {
                source-group имя_группы {
                    domain домен
                }
            }
        }
    }
}
```

Параметры

имя_группы

Множественный узел. Название группы.

домен

Название домена, который нужно включить в члены группы (например,numatech.ru).

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для включения домена в члены группы.

Форма **set** команды используется для включения указанного домена в указанную группу.

Форма **delete** команды используется для исключения указанного домена из указанной группы.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.40 service webproxy url-filtering squidguard source-group <имя_группы> ldap-group <имя_LDAP_группы>

Добавление пользователей, относящихся к данной группе пользователей LDAP, в члены указанной группы.

Синтаксис

```
set service webproxy url-filtering squidguard source-group <имя_группы> ldap-group <имя_группы_LDAP>

delete service webproxy url-filtering squidguard source-group <имя_группы> ldap-group <имя_группы_LDAP>

show service webproxy url-filtering squidguard source-group <имя_группы> ldap-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      url-filtering {
         squidguard {
            source-group имя_группы {
               ldap-group имя_группы_LDAP
            }
         }
      }
   }
}
```

Параметры

имя_группы

Множественный узел. Название группы.

имя_группы_LDAP

Имя группы пользователей LDAP, пользователей которой нужно включить в члены группы.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для включения пользователей, состоящих в данной группе пользователей LDAP, в члены указанной группы. Группировка пользователей LDAP должна осуществляться с использованием записей объектного класса (objectClass) posixGroup. Данная команда работает только при настроенной аутентификации на сервере LDAP, для всех пользователей, успешно прошедших аутентификацию.

Форма **set** команды используется для включения пользователей, состоящих в данной группе пользователей LDAP, в указанную группу.

Форма **delete** команды используется для исключения пользователей, состоящих в данной группе пользователей LDAP, из указанной группы.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.41 service webproxy url-filtering squidguard source-group <имя_группы> user <имя_пользователя>

Добавляет пользователя, успешно прошедшего аутентификацию, в члены указанной группы.

Синтаксис

```
set service webproxy url-filtering squidguard source-group <имя_группы> user <имя_пользователя>

delete service webproxy url-filtering squidguard source-group <имя_группы> user <имя_пользователя>

show service webproxy url-filtering squidguard source-group <имя_группы> user
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        url-filtering {
            squidguard {
                source-group имя_группы {
                    user имя_пользователя
                }
            }
        }
    }
}
```

Параметры

имя_группы

Множественный узел. Название группы.

имя_пользователя

Имя аутентифицированного пользователя, которого нужно включить в члены группы.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для включения указанного пользователя в члены группы. Данная команда работает при использовании любого типа аутентификации, для всех пользователей, успешно прошедших аутентификацию.

Форма **set** команды используется для включения пользователя в указанную группу.

Форма **delete** команды используется для исключения пользователя из указанной группы.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.42 service webproxy url-filtering squidguard time-period <имя_промежутка>

Объявляет (пустой) промежуток времени, который можно потом определить и использовать в правилах фильтрации.

Синтаксис

```
set service webproxy url-filtering squidguard time-period <имя_промежутка>
delete service webproxy url-filtering squidguard time-period <имя_промежутка>
show service webproxy url-filtering squidguard time-period <имя_промежутка>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      url-filtering {
         squidguard {
            time-period имя_промежутка {
            }
         }
      }
   }
}
```

Параметры

имя_промежутка

Название промежутка.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда позволяет создать пустой промежуток времени (контейнер), в который позднее можно включить метки времени, определяющие его длительность и/или момент актуальности.

Форма **set** команды используется для создания (пустого) промежутка времени с указанным именем.

Форма **delete** команды используется для уничтожения промежутка времени с указанным именем.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.43 service webproxy url-filtering squidguard time-period <имя_промежутка> days <день> time <время>

Задаёт моменты времени и/или периоды актуальности для указанного промежутка времени.

Синтаксис

```
set service webproxy url-filtering squidguard time-period <имя_промежутка> day <день> time <время>
delete service webproxy url-filtering squidguard time-period <имя_промежутка> day <день> time
show service webproxy url-filtering squidguard time-period <имя_промежутка> day <день> time
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      url-filtering {
         squidguard {
            time-period имя_промежутка {
               day день {
                  time время
               }
            }
         }
      }
   }
}
```

Параметры

имя_промежутка

Название используемого промежутка времени, объявленного заранее.

день

День (или дни), по наступлении которого (которых) указанный промежуток времени приобретает актуальность. Поддерживаются следующие значения:

Mon: указанный промежуток времени актуален по понедельникам.

Tue: указанный промежуток времени актуален по вторникам.

Wed: указанный промежуток времени актуален по средам.

Thu: указанный промежуток времени актуален по четвергам.

Fri: указанный промежуток времени актуален по пятницам.

Sat: указанный промежуток времени актуален по субботам.

workday: указанный промежуток времени актуален по будням.

weekend: указанный промежуток времени актуален по выходным (не праздничным) дням.

any: указанный промежуток времени актуален во все дни.

время

Период времени (диапазон) в пределах суток, в течение которого актуален указанный промежуток. Представление времени 24-часовое, формат диапазона чч:мм-чч:мм. Можно указать несколько диапазонов (в пределах суточного времени) в формате "чч:мм-чч:мм, чч:мм-чч:мм" (например, "09:00-14:00, 18:00-24:00"). Если не указан временной промежуток, то считается что правило действует весь день (00:00-24:00).

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для задания диапазона (диапазонов) актуальности указанного промежутка времени.

Форма **set** команды используется для задания дня (или дней) и суточного диапазона (диапазонов) актуальности указанного промежутка.

Форма **delete** команды используется для исключения из указанного промежутка всех меток и диапазонов времени.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.44 service webproxy url-filtering squidguard time-period <имя_периода> description <описание>

Задаёт текстовое описание указанного промежутка времени.

Синтаксис

```
set service webproxy url-filtering squidguard time-period <имя_периода> description <описание>

delete service webproxy url-filtering squidguard time-period <имя_периода> description

show service webproxy url-filtering squidguard time-period <имя_периода> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      url-filtering {
         squidguard {
            time-period имя_периода {
               description описание
            }
         }
      }
   }
}
```

Параметры

имя_периода

Название используемого промежутка времени, объявленного заранее.

описание

Краткое текстовое описание работы промежутка. Если описание содержит пробелы, то оно должно быть заключено в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

С помощью этой команды можно связать с указанным промежутком времени текстовую информацию, помогающую понять его предназначение.

Форма **set** команды используется для связывания указанного текстового описания с указанным промежутком времени.

Форма **delete** команды используется для исключения описания из указанного промежутка времени.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.45 service webproxy request-log logfile <режим>

Включение регистрации отчетов модуля веб-прокси в локальном файле регистрации.

Синтаксис

```
set service webproxy request-log logfile <режим>
delete service webproxy request-log logfile
show service webproxy request-log logfile
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      request-log {
         syslog {
            logfile режим
         }
      }
   }
}
```

Параметры

режим

Допустимые значения:

enable: журналирование в файл /var/log/squid/access.log включено.

disable: журналирование в файл отключено.

Значение по умолчанию

По умолчанию установлено значение disable.

Указания по использованию

Данная команда позволяет настроить регистрацию отчетов модуля веб-прокси в локальном файле. При включении журналирования с использованием данной команды в локальный файл будут записываться все запросы пользователей к модулю веб-прокси. Для просмотра отчетов используется команда эксплуатационного режима **show webproxy log**.

Форма **set** данной команды используется для включения журналирования в локальный файл.

Форма **delete** данной команды используется для удаления конфигурации.

Форма **show** данной команды используется для отображения конфигурации.

25.4.46 service webproxy request-log syslog

Включение регистрации отчетов модуля веб-прокси в системном журнале.

Синтаксис

```
set service webproxy request-log syslog
delete service webproxy request-log syslog
show service webproxy request-log syslog
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
```

```
        request-log {
            syslog {
            }
        }
    }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет настроить журналирование регистрации отчетов модуля веб-прокси в главном системном журнале регистрации.

Форма **set** данной команды используется для включения журналирования запросов к веб-прокси в главном системном журнале регистрации.

Форма **delete** данной команды используется для удаления конфигурации.

Форма **show** данной команды используется для отображения конфигурации.

25.4.47 service webproxy request-log syslog facility <источник>

Указание источника сообщений, от имени которого модуль веб-прокси будет отправлять сообщения в системный журнал.

Синтаксис

```
set service webproxy request-log syslog facility <источник>
delete service webproxy request-log syslog facility
show service webproxy request-log syslog facility
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        request-log {
            syslog {
                facility источник          }
        }
    }
}
```

Параметры

источник

Типы сообщений, которые будут отправляться в главный системный журнал. Поддерживаемые типы источников сообщений приведены в таблице типов источников сообщений.

Значение по умолчанию

По умолчанию используется источник «local4».

Указания по использованию

Данная команда позволяет настроить тип источника сообщений системы веб-прокси в системном журнале регистрации.

Форма **set** данной команды используется для указания типа источника сообщений.

Форма **delete** данной команды используется для удаления конфигурации.

Форма s**how** данной команды используется для отображения конфигурации.

25.4.48 service webproxy request-log syslog level <уровень>

Указание уровня серьезности сообщений модуля веб-прокси, которые будут регистрироваться в системном журнале.

Синтаксис

```
set service webproxy request-log syslog level <уровень>
delete service webproxy request-log syslog level
show service webproxy request-log syslog level
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      request-log {
         syslog {
            level уровень          }
      }
   }
}
```

Параметры

уровень

Наименьший уровень серьезности для сообщения журнала, которое будет записано. Поддерживаются значения err, warning, notice, info, debug. Разъяснение смысла этих уровней приведено в таблице уровней серьёзности сообщений.

Значение по умолчанию

По умолчанию используется уровень «notice».

Указания по использованию

Данная команда позволяет задать уровень серьезности сообщений службы веб-прокси, посылаемых в системный журнал. В настройках системного журнала должна быть настроена фиксация сообщений не ниже уровня серьезности сообщений, отправляемых веб-прокси. Уровень регистрации сообщений в системном журнале настраивается параметром **system syslog global facility <источник> level <уровень>** .

Форма **set** данной команды используется для указания уровня серьезности сообщений.

Форма **delete** данной команды используется для удаления конфигурации.

Форма **show** данной команды используется для отображения конфигурации.

25.4.49 service webproxy request-log sql-db db-name <имя>

Указание имени внешней базы данных для регистрации отчетов модуля веб-прокси.

Синтаксис

```
set service webproxy request-log sql-db db-name <имя>
```

```
delete service webproxy request-log sql-db db-name
show service webproxy request-log sql-db db-name
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        request-log {
            sql-db {
                db-name имя
            }
        }
    }
}
```

Параметры

имя

Имя базы данных, в которую будет происходить запись.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать имя базы данных при настройке регистрации отчетов модуля веб-прокси во внешней базе данных.

База данных должна быть заранее создана. В том случае если база данных пуста, то она будет автоматически проинициализирована. Для этого необходимо, чтобы пользователь, который указан в настройке, обладал привилегией CREATE.

Форма **set** данной команды используется для указания имени базы данных.

Форма **delete** данной команды используется для удаления конфигурации.

Форма **show** данной команды используется для отображения конфигурации.

25.4.50 service webproxy request-log sql-db db-type <имя>

Указание типа СУБД, используемой для регистрации отчетов системы веб-прокси.

Синтаксис

```
set service webproxy request-log sql-db db-type <тип>
delete service webproxy request-log sql-db db-type
show service webproxy request-log sql-db db-type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        request-log {
            sql-db {
                db-type тип
```

```
            }
        }
    }
}
```

Параметры

тип

Тип используемой СУБД. В настоящий момент поддерживается работа СУБД MySQL. Допустимое значение mysql.

Значение по умолчанию

По умолчанию установлено значение mysql.

Указания по использованию

Данная команда позволяет указать тип используемой СУБД.

Форма **set** данной команды используется для указания типа СУБД.

Форма **delete** данной команды используется для удаления конфигурации.

Форма **show** данной команды используется для отображения конфигурации.

25.4.51 service webproxy request-log sql-db host <адрес>

Указание адреса или символьного имени сервера БД для подключения.

Синтаксис

```
set service webproxy request-log sql-db host <адрес>
delete service webproxy request-log sql-db host
show service webproxy request-log sql-db host
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        request-log {
            sql-db {
                host адрес
            }
        }
    }
}
```

Параметры

адрес

IPv4-адрес или символьное имя сервера БД.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать адрес или символьное имя сервера БД.

Форма **set** данной команды используется для указания адреса для подключения.

Форма delete данной команды используется для удаления конфигурации.

Форма **show** данной команды используется для отображения конфигурации.

25.4.52 service webproxy request-log sql-db username <имя_пользователя>

Указание имени пользователя, от имени которого будет осуществляться запись в БД.

Синтаксис

```
set service webproxy request-log sql-db username <имя_пользователя>
delete service webproxy request-log sql-db username
show service webproxy request-log sql-db username
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      request-log{
         sql-db {
            username имя_пользователя
         }
      }
   }
}
```

Параметры

имя_пользователя

Имя пользователя, от имени которого будет осуществляться запись в БД.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать имя пользователя, от имени которого будет осуществляться запись в БД. Указанный пользователь должен обладать правами на удаленный доступ, а также иметь привилегии CREATE и INSERT. В том случае если указанный пользователь не обладает привилегией CREATE, используемая база данных должна быть заранее инициализирована.

Форма **set** данной команды используется для указания имени пользователя.

Форма **delete** данной команды используется для удаления конфигурации.

Форма **show** данной команды используется для отображения конфигурации.

25.4.53 service webproxy request-log sql-db password <пароль>

Указание пароля пользователя.

Синтаксис

```
set service webproxy request-log sql-db password <пароль>
delete service webproxy request-log sql-db password
show service webproxy request-log sql-db password
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        request-log{
            sql-db {
                password пароль
            }
        }
    }
}
```

Параметры

пароль

Пароль пользователя.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать пароль пользователя, от имени которого будет осуществляться запись в БД.

Форма **set** данной команды используется для указания пароля пользователя.

Форма **delete** данной команды используется для удаления конфигурации.

Форма **show** данной команды используется для отображения конфигурации.

25.4.54 service webproxy icap filter <режим>

Настройка режима фильтрации запросов/ответов.

Синтаксис

```
set service webproxy icap filter <режим>
delete service webproxy icap filter
show service webproxy icap filter
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        icap {
            filter режим
        }
    }
}
```

Параметры

режим

Допустимые значения:

request: режим фильтрации с обработкой запросов.

response: режим фильтрации с обработкой ответов.

Значение по умолчанию

По умолчанию задано значение **response**.

Указания по использованию

Настройка режима фильтрации запросов/ответов.

Форма **set** команды используется для выбора режима фильтрации запросов или ответов веб-прокси.

Форма **delete** команды используется для восстановления режима фильтрации, установленного по умолчанию.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.55 service webproxy icap persistent-connections <режим>

Настройка режима постоянного соединения с сервером ICAP.

Синтаксис

```
set service webproxy icap persistent-connections <режим>
delete service webproxy icap persistent-connections
show service webproxy icap persistent-connections
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      icap {
         persistent-connections режим
      }
   }
}
```

Параметры

режим

Допустимые значения:

true: Включить режим постоянного соединения с сервером ICAP.

false: Отключить режим постоянного соединения с сервером ICAP.

Значение по умолчанию

По умолчанию постоянное соединение с сервером ICAP отключено.

Указания по использованию

Должно быть установлено одно из значений false/true.

Форма **set** команды используется для настройки режима постоянного соединения с сервером ICAP.

Форма **delete** команды используется для восстановления режима соединения, установленного по умолчанию.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.56 service webproxy icap preview <режим>

Настройка режима preview для сервера ICAP.

Синтаксис

```
set service webproxy icap preview <режим>
delete service webproxy icap preview
show service webproxy icap preview
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      icap {
         preview режим
      }
   }
}
```

Параметры

режим

Допустимые значения:

enable: Включить режим preview для сервера ICAP.

disable: Отключить режим preview для сервера ICAP.

Значение по умолчанию

По умолчанию постоянное соединение с сервером ICAP включено.

Указания по использованию

Должно быть установлено одно из значений enable/disable.

Форма **set** команды используется для настройки режима preview для сервера ICAP.

Форма **delete** команды используется для восстановления режима, принятого по умолчанию.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.57 service webproxy icap send-client-ip <режим>

Настройка указания IP-адреса клиента в запросе ICAP.

Синтаксис

```
set service webproxy icap send-client-ip <режим>
delete service webproxy icap send-client-ip
show service webproxy icap send-client-ip
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      icap {
         send-client-ip режим
      }
   }
```

```
}
```

Параметры

режим

Допустимые значения:

true: IP-адрес клиента в запросе передаётся.

false: IP-адрес клиента в запросе НЕ передаётся.

Значение по умолчанию

По умолчанию IP-адрес клиента в запросе ICAP передаётся (true).

Указания по использованию

Должно быть установлено одно из значений true/false.

Форма **set** команды используется для настройки передачи или запрета передачи IP-адреса клиента в запросах ICAP.

Форма **delete** команды используется для восстановления режима, принятого по умолчанию.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.58 service webproxy icap server-address <ipv4-адрес>

Указание адреса сервера ICAP.

Синтаксис

```
set service webproxy icap server-address <ipv4_адрес>
delete service webproxy icap server-address
show service webproxy icap server-address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      icap {
         server-address ipv4-адрес
      }
   }
}
```

Параметры

ipv4_адрес

IPv4 адрес сервера ICAP.

Значение по умолчанию

Не установлено.

Указания по использованию

Форма **set** команды используется для указания IP-адреса сервера ICAP.

Форма **delete** команды используется для удаления имеющейся настройки.

Форма **show** команды используется для просмотра текущего состояния настройки.

25.4.59 service webproxy icap server-port <порт>

Указание порта сервера ICAP.

Синтаксис

```
set service webproxy icap server-port <порт>
delete service webproxy icap server-port
show service webproxy icap server-port
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      icap {
         server-port порт
      }
   }
}
```

Параметры

порт

Порт сервера ICAP. Диапазон допустимых значений составляет 1-65535

Значение по умолчанию

Не установлено.

Указания по использованию

Форма **set** команды используется для указания порта сервера ICAP.

Форма **delete** команды используется для удаления имеющейся настройки.

Форма **show** команды используется для просмотра текущего состояния настройки.

25.4.60 service webproxy icap service-name <имя>

Указание имени сервера ICAP.

Синтаксис

```
set service webproxy icap service-name <имя>
delete service webproxy icap service-name
show service webproxy icap service-name
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      icap {
         service-name имя
      }
   }
}
```

Параметры

имя

Имя сервера ICAP.

Значение по умолчанию

Не установлено.

Указания по использованию

Форма **set** команды используется для указания имени сервера ICAP.

Форма **delete** команды используется для удаления имеющейся настройки.

Форма **show** команды используется для просмотра текущего состояния настройки.

25.4.61 service webproxy listen-address <ipv4_адрес> enable-ssl

Включает режим проксирования соединений SSL.

Синтаксис

```
set service webproxy listen-address <ipv4_адрес> enable-ssl
delete service webproxy listen-address <ipv4_адрес> enable-ssl
show service webproxy listen-address <ipv4_адрес>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      listen-address ipv4_адрес {
         enable-ssl
      }
   }
}
```

Параметры

ipv4_адрес

IPv4-адрес сетевого интерфейса, на котором веб-прокси ожидает соединения.

Значение по умолчанию

Режим проксирования соединений SSL отключен.

Указания по использованию

Эта команда предназначена для включения режима проксирования соединений SSL. При включении режима проксирования необходимо указать сертификат УЦ, который будет использоваться прокси-сервером. При использовании прозрачного режима проксирования трафик HTTPS будет автоматически перенаправляться на порт, прослушиваемый прокси-сервером.

Форма **set** команды используется для включения режима проксирования соединений SSL.

Форма **delete** команды используется для выключения режима проксирования соединений SSL.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.62 service webproxy ssl disable-verify

Отключить проверку сертификатов удаленных серверов при включенном проксировании соединений SSL.

Синтаксис

```
set service webproxy ssl disable-verify
delete service webproxy ssl disable-verify
show service webproxy ssl
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      ssl {
         disable-verify      }
   }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

По умолчанию проверка сертификатов удаленных серверов включена.

Указания по использованию

Эта команда предназначена для отключения проверки сертификатов удаленных серверов при включенном проксировании соединений SSL.

В противном случае прокси-сервер осуществляет проверку того, что сертификат удаленного сервера действующий и подписан доверенным УЦ, при этом прокси-сервер считает доверенными только те УЦ, которые известны модулю PKI (например, импортированы в модуль PKI, узел конфигурации pki). Таким образом, для корректной работы, в случае если проверка сертификатов удаленных серверов включена, необходимо импортировать сертификаты доверенных УЦ при помощи команды pki import ca.

ПРИМЕЧАНИЕ В том случае если проверка сертификатов удаленных серверов отключена, будут приниматься все сертификаты, включая те, которые не прошли проверку. В связи с этим отключение проверки сертификатов удаленных серверов строго не рекомендуется, так как в этом случае нельзя гарантировать надежность серверов и безопасность устанавливаемых соединений.

Форма **set** команды используется для отключения проверки сертификатов удаленных серверов.

Форма **delete** команды используется для удаления настройки и восстановления значения, принятого по умолчанию.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.63 service webproxy ssl x509-cert <имя_сертификата>

Указание имени сертификата удостоверяющего центра, который будет использоваться прокси-сервером.

Синтаксис

```
set service webproxy ssl x509-cert <имя_сертификата>
delete service webproxy ssl x509-cert
show service webproxy ssl x509-cert
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      ssl {
         x509-cert имя_сертификата
      }
```

```
    }
}
```

Параметры

имя_сертификата

Обязательный. Имя сертификата удостоверяющего центра.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для указания сертификата УЦ, который будет использоваться прокси-сервером. Сертификат должен быть создан или импортирован ранее в систему управления ключами, узел pki. Для выпуска сертификатов, используемых при перехвате SSL/TLS соединения, для данного УЦ требуется наличие закрытого ключа.

Форма **set** команды используется указания имени сертификата УЦ.

Форма **delete** команды используется для удаления имени сертификата УЦ.

Форма **show** команды используется для просмотра конфигурации имени сертификата УЦ, используемого прокси-сервером.

25.4.64 service webproxy url-filtering ssl block-server [name <домен> | regex <выражение>]

Используется для задания домена, либо регулярного выражения, доступ к которым блокируется прокси сервером.

Синтаксис

```
set webproxy url-filtering ssl block-server <размер>
delete webproxy url-filtering ssl block-server
show webproxy url-filtering ssl block-server
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      url-filtering {
         ssl {
            block-server name домен| regex выражение
         }
      }
   }
}
```

Параметры

name

Множественный узел. Доменное имя веб-сайта, доступ к которому должен быть заблокирован на прокси сервере.

regex

Множественный узел. Регулярное выражение, которое описывает один или группу доменов, доступ к которому должен быть заблокирован на прокси сервере.

Значение по умолчанию

Отсутствует

Указания по использованию

Прокси сервер получает доменное имя веб-сайта, к которому обращается клиент одним из следующих способов для HTTPS трафика:

- Поле SNI в сообщении Client Hello при установлении SSL/TLS соединения.
- В полях CN и SubjectAltName сертификата веб-сайта в сообщении Server Hello.

При совпадении доменного имени сайта с одним из заданных значений, последующий обмен сообщениями между клиентом и веб-сайтом будут заблокированы.

Форма **set** команды используется для задания домена, либо регулярного выражения, доступ к которым блокируется прокси сервером.

Форма **delete** команды используется для удаления доменного имени веб-сервера.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.65 service webproxy url-filtering ssl bump-server [name <домен> | regex <выражение>]

Настройка перехвата SSL/TLS соединения между веб-сайтом и клиентом для последующей настройки фильтрации.

Синтаксис

```
set webproxy url-filtering ssl bump-server <размер>
delete webproxy url-filtering ssl bump-server
show webproxy url-filtering ssl bump-server
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      url-filtering {
         ssl {
            bump-server name домен| regex выражение
         }
      }
   }
}
```

Параметры

name

Множественный узел. Доменное имя веб-сайта, для которого производится перехват SSL/TLS соединения на прокси сервере с последующей подменой серверного сертификата, отдаваемого клиенту.

regex

Множественный узел. Регулярное выражение, для которого производится перехват SSL/TLS соединения на прокси сервере с последующей подменой серверного сертификата, отдаваемого клиенту.

Значение по умолчанию

Отсутствует

Указания по использованию

Прокси сервер получает доменное имя веб-сайта, к которому обращается клиент одним из следующих способов для HTTPS трафика:

- Поле SNI в сообщении Client Hello при установлении SSL/TLS соединения.
- В полях CN и SubjectAltName сертификата веб-сайта в сообщении Server Hello.

При совпадении доменного имени сайта с одним из заданных значений, прокси сервер самостоятельно устанавливает SSL/TLS соединение с веб-сервером. С клиентом устанавливается SSL/TLS соединение, используя сгенерированный сертификат на прокси сервере. Этот сертификат подписывается УЦ, который настроен в атрибуте **service webproxy ssl x509-cert <имя_сертификата>.** После перехвата SSL/TLS соединения, для данного домена или группы доменов возможно использование правил фильтрации веб-контента, задаваемых в узле конфигурации **service webproxy url-filtering squidguard.**

Форма **set** используется для настройки перехвата SSL/TLS соединения между веб-сайтом и клиентом.

Форма **delete** команды используется для удаления доменного имени веб-сервера.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.66 service webproxy cache-size <размер>

Задаёт объём кэша - хранилища для временного хранения содержимого.

Синтаксис

```
set service webproxy cache-size <размер>
delete service webproxy cache-size
show service webproxy cache-size
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      cache-size размер
   }
}
```

Параметры

размер

Объём дискового пространства, в МБайт, отведённого под кэш. Диапазон значений от 0 до 4294967295, причём значение 0 выключает кэширование.

Значение по умолчанию

По умолчанию объём кэша установлен в 0 МБайт, т.е. кэширование не производится.

Указания по использованию

Эта команда предназначена для включения/выключения кэширования веб-данных и указания объёма хранилища для их временного хранения.

Форма **set** команды включает/выключает кэширование, изменяет объём кэша.

Форма **delete** восстанавливает объём кэша по умолчанию (и выключает кэширование, если объём по умолчанию выставлен в 0).

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.67 service webproxy domain-noncache <домен>

Выключает кэширование данных, полученных с указанного домена в ответ на запросы пользователей.

Синтаксис

```
set service webproxy domain-noncache <домен>
delete service webproxy domain-noncache <домен>
show service webproxy domain-noncache
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      domain-noncache домен
   }
}
```

Параметры

домен

Множественный узел. Имя домена, данные с которого в кэш помещаться не будут.

Значение по умолчанию

Если домен в команде не указан, то в кэш помещается всё содержимое, не противоречащее другим ограничениям.

Указания по использованию

Эта команда предназначена для указания домена, кэширование ответов для которого не производится.

Форма **set** команды используется для указания домена, данные с которого в кэш помещать не надо.

Форма **delete** команды используется для восстановления кэширования данных с указанного домена.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.68 service webproxy maximum-object-size <размер>

Прокси будет помещать в кэш объекты с размером не больше указанного.

Синтаксис

```
set service webproxy maximum-object-size <размер>
delete service webproxy maximum-object-size
show service webproxy maximum-object-size
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      maximum-object-size размер
   }
}
```

Параметры

размер

Максимальный размер объекта (в килобайтах).

Значение по умолчанию

Прокси не ограничивает максимальный размер объектов, помещаемых в кэш.

Указания по использованию

Эта команда предназначена для ограничения «сверху» размеров объектов, помещаемых в кэш. Объекты с размером, превышающим указанный, в кэш не попадут.

Форма **set** команды используется для задания максимального размера помещаемых в кэш объектов.

Форма **delete** команды используется для восстановления поведения по умолчанию.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.69 service webproxy minimum-object-size <размер>

Прокси будет помещать в кэш объекты с размером не меньше указанного.

Синтаксис

```
set service webproxy minimum-object-size <размер>
delete service webproxy minimum-object-size
show service webproxy minimum-object-size
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      minimum-object-size размер
   }
}
```

Параметры

размер

Минимальный размер объекта (в килобайтах).

Значение по умолчанию

Прокси не ограничивает минимальный размер объектов, помещаемых в кэш.

Указания по использованию

Эта команда предназначена для ограничения «снизу» размеров объектов, помещаемых в кэш. Объекты с размером меньше указанного в кэш не попадут.

Форма **set** команды используется для задания минимального размера помещаемых в кэш объектов.

Форма **delete** команды используется для восстановления поведения по умолчанию.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.70 service webproxy authentication method <метод>

Указание используемого метода аутентификации пользователей прокси.

Синтаксис

```
set service webproxy authentication method <метод>
delete service webproxy authentication method
show service webproxy authentication method
```

Режим команды

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      authentication {
         method метод
      }
   }
}
```

Параметры

метод

Используемый метод аутентификации пользователей прокси. Допустимые значения:

none: Аутентификация пользователей не используется. Установлен по умолчанию.

ldap: Аутентификация на основе протокола LDAP.

ПРИМЕЧАНИЕ: При использовании метода аутентификации на основе протокола LDAP, в контроллере домена каждому аутентифицируемому пользователю необходимо добавить атрибут *uid*. Значение этого атрибута используется в качестве логина.

ntlm: Аутентификация на основе протокола NTLM.

radius: Аутентификация через сервер RADIUS.

Значение по умолчанию

По умолчанию аутентификация пользователей не используется.

Указания по использованию

Эта команда предназначена для указания метода аутентификации пользователей прокси. По умолчанию аутентификация отключена, а прокси-сервер функционирует в прозрачном режиме. При включении аутентификации пользователей прокси, необходимо отключить прозрачный режим, для этого используется команда .

При использовании непрозрачного режима работы необходимо указывать параметры прокси-сервера в настройках клиентского ПО.

Форма **set** этой команды используется для указания метода аутентификации.

Форма **delete** этой команды используется для возвращения параметру значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации.

25.4.71 service webproxy authentication ntlm name <имя>

Указание имени компьютера в домене.

Синтаксис

```
set service webproxy authentication ntlm name <имя>
delete service webproxy authentication ntlm name
show service webproxy authentication ntlm name
```

Режим команды

Режим настройки.

Ветвь конфигурации

```
service {
```

```
webproxy {
    authentication {
        ntlm {
            name имя
        }
    }
}}
```

Параметры

имя

Имя NetBIOS компьютера в домене.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для указания NetBIOS имени, по которому будет доступен Numa Edge.

Форма **set** этой команды используется для указания имени компьютера в домене.

Форма **delete** этой команды используется для возвращения параметру значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации.

25.4.72 service webproxy authentication ntlm password <пароль>

Указание пароля для учетной записи пользователя, которая используется для авторизации в домене.

Синтаксис

```
set service webproxy authentication ntlm password <пароль>
delete service webproxy authentication ntlm password
show service webproxy authentication ntlm password
```

Режим команды

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        authentication {
            ntlm {
                password пароль          }       }
    }
}
```

Параметры

пароль

Пароль для учетной записи пользователя, которая используется для авторизации в домене.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда позволяет указать пароль учетной записи пользователя, который используется для авторизации в домене.

В домене должна быть создана учетная запись пользователя с правами на ввод компьютеров в домен. Данная учетная запись используется для авторизации в домене.

Форма **set** этой команды используется для указания пароля.

Форма **delete** этой команды используется для удаления текущей конфигурации пароля.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации.

25.4.73 service webproxy authentication ntlm pdc <адрес>

Указание IP-адреса или имени контроллера домена.

Синтаксис

```
set service webproxy authentication ntlm pdc <адрес>
delete service webproxy authentication  ntlm pdc
show service webproxy authentication  ntlm pdc
```

Режим команды

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      authentication {
         ntlm {
            pdc адрес
         }
      }
   }
}
```

Параметры

адрес

IP-адрес или символьное имя контроллера домена.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для указания адреса или имени контроллера домена.

Форма **set** этой команды используется для указания адреса или имени контроллера домена.

Форма **delete** этой команды используется для возвращения параметру значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации.

25.4.74 service webproxy authentication ntlm user <имя_пользователя>

Указание имени пользователя для авторизации в домене.

Синтаксис

```
set service webproxy authentication ntlm user <имя_пользователя>
delete service webproxy authentication ntlm user
show service webproxy authentication ntlm user
```

Режим команды

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        authentication {
            ntlm {
                user имя_пользователя          }
        }
    }
}
```

Параметры

имя_пользователя

Имя пользователя для авторизации в домене.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для указания имени пользователя для авторизации в домене.

В домене должна быть создана учетная запись пользователя с правами на ввод компьютеров в домен. Данная учетная запись используется для авторизации в домене.

Форма **set** этой команды используется для указания имени пользователя для авторизации в домене.

Форма **delete** этой команды используется для возвращения параметру значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации.

25.4.75 service webproxy authentication ntlm workgroup <имя_домена>

Указание имени домена.

Синтаксис

```
set service webproxy authentication ntlm workgroup <имя_домена>
delete service webproxy authentication ntlm workgroup
show service webproxy authentication ntlm workgroup
```

Режим команды

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        authentication {
            ntlm {
                workgroup имя_домена          }
        }
    }
}
```

Параметры

имя_домена

Имя домена.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для указания имени NetBIOS домена.

Форма **set** этой команды используется для указания имени домена.

Форма **delete** этой команды используется для возвращения параметру значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации.

25.4.76 service webproxy authentication radius address <адрес>

Указание IP-адреса сервера RADIUS для аутентификации в веб-прокси.

Синтаксис

```
set service webproxy authentication radius address адрес
delete service webproxy authentication radius address
show service webproxy authentication radius address
```

Режим команды

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      authentication {
         radius {
            address адрес
         }
      }
   }
}
```

Параметры

ip_адрес

IP-адрес сервера RADIUS.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для указания IP-адреса сервера RADIUS для аутентификации в веб-прокси.

Форма **delete** этой команды используется для удаления настройки.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации.

25.4.77 service webproxy authentication radius port <порт>

Указание порта сервера RADIUS для аутентификации в веб-прокси.

Синтаксис

```
set service webproxy authentication radius port <порт>
delete service webproxy authentication radius port
show service webproxy authentication radius port
```

Режим команды

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        authentication {
            radius {
                port порт
            }
        }
    }
}
```

Параметры

порт

Порт сервера RADIUS. Значение должно лежать в диапазоне 1-65535.

Значение по умолчанию

По умолчанию используется порт 1821.

Указания по использованию

Форма **set** этой команды используется для указания порта сервера RADIUS для аутентификации в веб-прокси.

Форма **delete** этой команды используется для удаления настройки.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации.

25.4.78 service webproxy authentication radius digest-type <алгоритм>

Указание алгоритма хеширования для протокола RADIUS, используемого для аутентификации веб-прокси.

Синтаксис

```
set service webproxy authentication radius digest-type <алгоритм>
delete service webproxy authentication radius digest-type
show service webproxy authentication radius digest-type
```

Режим команды

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        authentication {
            radius {
                digest-type алгоритм
            }
        }
    }
}
```

Параметры

алгоритм

Алгоритм хеширования для протокола RADIUS. Допустимые значения: md5, gosthash-2012-256.

Значение по умолчанию

По умолчанию используется алгоритм gosthash-2012-256.

Указания по использованию

Форма **set** этой команды используется для указания алгоритма хеширования для протокола RADIUS.

Форма **delete** этой команды используется для удаления настройки.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации.

25.4.79 service webproxy authentication radius secret <ключ>

Указание разделяемого ключа для аутентификации в веб-прокси через сервер RADIUS.

Синтаксис

```
set service webproxy authentication radius secret <ключ>delete service webproxy authentication radius secretshow service webproxy authentication radius secret
```

Режим команды

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        authentication {
            radius {
                secret ключ
            }
        }
    }
}
```

Параметры

ключ

Разделяемый ключ для аутентификации через сервер RADIUS.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для указания разделяемого ключа для аутентификации в веб-прокси через сервер RADIUS.

Форма **delete** этой команды используется для удаления настройки.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации.

25.4.80 service webproxy append-domain <домен>

Указанное доменное имя будет присоединяться к каждому URL, доменная часть которого не содержит точек, перед его дальнейшей обработкой.

Синтаксис

```
set service webproxy append-domain <домен>
```

```
delete service webproxy append-domain
show service webproxy append-domain
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      append-domain домен
   }
}
```

Параметры

домен

Имя домена, которое будет присоединяться к доменной части URL.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для присоединения через точку указанного доменного имени к доменной части URL, не содержащей точек. Например, если в рассматриваемой команде указано доменное имя "numatech.ru", а запрос пользователя обращается по URL "www/abc.php", то в результате присоединения в дальнейшую обработку пойдёт URL "www.numatech.ru/abc.php".

Форма **set** команды используется для задания доменного имени, которое будет использовано для таких присоединений.

Форма **delete** команды используется для стирания доменного имени для присоединений и таким образом выключает их.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.81 service webproxy access-ports [http <порт> | https <порт>]

Задание списка разрешенных портов назначения, с которыми может устанавливать соединение клиент, используя заданный протокол.

Синтаксис

```
set service webproxy access-ports [http <порт> | https <порт>]
delete service webproxy access-ports
show service webproxy access-ports
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      access-ports http порт | https порт
   }
}
```

Параметры

порт

Множественный узел. Значение или диапазон TCP портов назначения.

Значение по умолчанию

Для протокола HTTP используются значения: **21,70,80,210,280,443,488,591,777,1025-65535**. Для протокола HTTPS: **443**.

Указания по использованию

Задание списка разрешенных портов назначения, с которыми может устанавливать соединение клиент, используя заданный протокол.

Форма **set** команды используется для задания списка разрешенных портов назначения, с которыми может устанавливать соединение клиент, используя заданный протокол.

Форма **delete** команды восстанавливает значения по умолчанию.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.82 service webproxy forwarded-for <режим>

Настройка X-Forwarded-For заголовка.

Синтаксис

```
set service webproxy forwarded-for <режим>
delete service webproxy forwarded-for
show service webproxy forwarded-for
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      forwarded-for режим
   }
}
```

Параметры

режим

Доступна настройка одного из следующих значений:

- **on:** Прокси-сервер добавляет в поле X-Forwarded-For IP-адрес клиента;
- **off:** IP-адрес клиента указывается как неизвестный;
- **transparent:** Данное поле передается прокси-сервером без изменений;
- **delete:** Если поле X-Forwarded-For было установлено, прокси сервер его удалит;
- **truncate:** Если в поле X-Forwarded-For были установлены другие значения, прокси сервер удалит их и добавит только IP-адрес клиента.

Значение по умолчанию

По умолчанию используется значение **off**.

Указания по использованию

Заголовок X-Forwarded-For является нестандартным для протокола HTTP. Данный заголовок используется для идентификации клиента, который обращается к веб-серверу через прокси-сервер или балансировщик нагрузки, в котором содержится IP-адрес клиента.

Форма **set** команды используется для задания режима перенаправление заголовка X-Forwarded-For.

Форма **delete** команды восстанавливает поведение по умолчанию.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.83 service webproxy host-verify-policy <тип_верификации>

Настройка действия в случае ошибки верификации заголовка «Host» (или SNI для TLS) и IP-адреса назначения клиентского запроса в режиме прозрачного прокси.

Синтаксис

```
set service webproxy host-verify-policy <тип_верификации>
delete service webproxy host-verify-policy
show service webproxy host-verify-policy
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      host-verify-policy тип_верификации
   }
}
```

Параметры

тип_верификации

Допустимые значения:

strict: В случае ошибки верификации, веб-прокси не передает запрос клиента на веб-сервер, а отвечает HTTP/409 Conflict. Сообщение об ошибке верификации записывается в журнал.

warning: В случае ошибки верификации, веб-прокси не прерывает запрос клиента, только записывает сообщение об ошибке в журнал.

Значение по умолчанию

strict В случае ошибки верификации, веб-прокси не передает запрос клиента на веб-сервер, а отвечает HTTP/409 Conflict. Сообщение об ошибке верификации записывается в журнал.

Указания по использованию

Верификация заголовка «Host» (или SNI для TLS) и IP-адреса производится веб-прокси вне зависимости он значений данного аргумента, согласно требованиям RFC 2616. Под верификацией понимается процесс преобразования доменного имени из заголовка «Host» (или SNI для TLS) в IP-адрес и последующим сравнением с IP-адресом назначения пакета. Преобразование производится веб-прокси через службу DNS. Ошибкой верификации считается несовпадение данных IP-адресов.

Форма **set** этой команды используется для настройки действия в случае ошибки верификации заголовка «Host» (или SNI для TLS) и IP-адреса назначения клиентского запроса в режиме прозрачного прокси.

Форма **delete** этой команды используется для восстановления действия по умолчанию.

Форма **show** этой команды используется для просмотра текущего действия в случае ошибки верификации заголовка «Host» (или SNI для TLS)в режиме прозрачного прокси.

25.4.84 service webproxy identity admin-email <адрес>

Задаёт адрес электронного почтового ящика администратора веб-прокси.

Синтаксис

```
set service webproxy identity admin-email <адрес>
delete service webproxy identity admin-email
show service webproxy identity admin-email
```

Режим команды

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        identity {
            admin-email адрес
        }
    }
}
```

Параметры

адрес

Адрес электронного почтового ящика администратора веб-прокси.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для установки адреса электронного почтового ящика человека, ответственного за работу веб-прокси. На этот адрес прокси будет отправлять служебные сообщения о своей работе, также он может отображаться на служебных страницах, выдаваемых прокси в особых случаях.

Форма **set** команды используется для задания адреса электронного почтового ящика.

Форма **delete** команды используется для стирания адреса электронного почтового ящика.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.85 service webproxy identity hostname <имя>

Задаёт имя системы, которым веб-прокси будет обозначать себя.

Синтаксис

```
set service webproxy identity hostname <имя>
delete service webproxy identity hostname
show service webproxy identity hostname
```

Режим команды

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        identity {
            hostname имя
        }
    }
}
```

Параметры

имя

Сетевое имя системы.

Значение по умолчанию

В том случае если значение для данного параметра явно не указано, используется имя Numa_Edge.

Указания по использованию

Эта команда предназначена для установки имени системы, которым веб-прокси будет обозначать себя в сообщениях об ошибках.

Форма **set** команды используется для задания сетевого имени системы.

Форма **delete** команды используется для стирания сетевого имени системы.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.86 service webproxy listen-address <ipv4_адрес>

Задаёт адрес IPv4 сетевого интерфейса, на котором веб-прокси будет ожидать соединения.

Синтаксис

```
set service webproxy listen-address <ipv4_адрес>
delete service webproxy listen-address <ipv4_адрес>
show service webproxy listen-address <ipv4_адрес>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      listen-address ipv4_адрес {
      }
   }
}
```

Параметры

ipv4_адрес

Множественный узел. IPv4-адрес интерфейса, на котором прокси будет ожидать соединения.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда предназначена для привязки программы-сервера веб-прокси к интерфейсу с указанным в команде адресом IP. По соображениями безопасности следует избегать настройки прокси на ожидание соединений на интерфейсах, не являющихся "внутренними" (обращёнными в локальную сеть), так как прокси по определению скрывает IP-адрес и иные данные своих клиентов, чем могут воспользоваться злоумышленники и в результате чего "снаружи" их действия будут выглядеть исходящими от вашей сети. Тем не менее защититься от этого можно и другими средствами, например, настройкой доступа к прокси, скажем, при помощи групп пользователей (source groups) или фаервола.

Форма **set** команды используется для задания адреса для ожидания соединений программой-сервером веб-прокси.

Форма **delete** команды используется для исключения указанного адреса из перечня тех, на которых прокси ожидает соединения. Последний в перечне адрес при работающем прокси убрать не получится - хотя бы один адрес должен присутствовать всегда.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.87 service webproxy listen-address <ipv4_адрес> disable-transparent

Выключает "прозрачный" режим работы для соединений, поступающих на интерфейс Numa Edge с указанным адресом.

Синтаксис

```
set service webproxy listen-address <ipv4_адрес> disable-transparent
delete service webproxy listen-address <ipv4_адрес> disable-transparent
show service webproxy listen-address <ipv4_адрес>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      listen-address ipv4_адрес {
         disable-transparent
      }
   }
}
```

Параметры

i*pv4_адрес*

IPv4-адрес сетевого интерфейса, на котором веб-прокси ожидает соединения.

Значение по умолчанию

"Прозрачный" режим работы включён.

Указания по использованию

Эта команда предназначена для выключения "прозрачного" режима работы прокси для запросов, приходящих на связанный с указанным IP-адресом сетевой интерфейс системы Numa Edge.

ПРЕДУПРЕЖДЕНИЕ При настройке webproxy по умолчанию устанавливается прозрачный режим работы. Для корректной работы webproxy в прозрачном режиме также необходимо вручную настроить NAT.

Форма **set** команды используется для выключения "прозрачного" режима работы прокси.

Форма **delete** команды используется для включения обратно "прозрачного" режима.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.88 service webproxy listen-address <ipv4-адрес> http-port <порт>

Задаёт отличный от значения по умолчанию номер порта для указанного IPv4-адреса прокси, используемого для HTTP трафика.

Синтаксис

```
set service webproxy listen-address <ipv4-адрес> http-port <порт>
delete service webproxy listen-address <ipv4-адрес> http-port
show service webproxy listen-address <ipv4-адрес> http-port
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   webproxy {
      listen-address ipv4_адрес {
         port порт
```

```
        }
    }
}
```

Параметры

ipv4-адрес

IPv4-адрес сетевого интерфейса, на котором веб-прокси ожидает соединения.

порт

Номер TCP-порта, на котором программа-сервер веб-прокси будет ожидать соединения.

Значение по умолчанию

По умолчанию используется значение 3128.

Указания по использованию

Эта команда предназначена для перенастройки прокси на ожидание соединений по другому порту, отличному от используемого по умолчанию для HTTP трафика. Перенастройка выполняется только для сетевого интерфейса, связанного с указанным IP-адресом.

Форма **set** команды используется для задания нового порта для ожидания входящих соединений в связке указанным IP-адресом.

Форма **delete** команды используется для переноса ожидания обратно на порт по умолчанию.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.89 service webproxy listen-address <ipv4_адрес> https-port <порт>

Задаёт отличный от значения по умолчанию номер порта для указанного IPv4-адреса прокси, используемого для HTTPS трафика.

Синтаксис

```
set service webproxy listen-address <ipv4_адрес> https-port <порт>
delete service webproxy listen-address <ipv4_адрес> https-port
show service webproxy listen-address <ipv4_адрес> https-port
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    webproxy {
        listen-address ipv4_адрес {
            https-port порт
        }
    }
}
```

Параметры

ipv4-адрес

IPv4-адрес сетевого интерфейса, на котором веб-прокси ожидает соединения.

порт

Номер TCP-порта, на котором программа-сервер веб-прокси будет ожидать соединения.

Значение по умолчанию

По умолчанию используется значение 3129.

Указания по использованию

Эта команда предназначена для перенастройки прокси на ожидание соединений по другому порту, отличному от используемого по умолчанию для HTTPS трафика. Перенастройка выполняется только для сетевого интерфейса, связанного с указанным IP-адресом.

Форма **set** команды используется для задания нового порта для ожидания входящих соединений в связке указанным IP-адресом.

Форма **delete** команды используется для переноса ожидания обратно на порт по умолчанию.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

25.4.90 service webproxy restart

Перезапускает процесс веб-прокси.

Синтаксис

```
service webproxy restart
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Указания по использованию

Эта команда предназначена для перезапуска работающего процесса веб-прокси.

Примеры

Перезапуск процесса веб-прокси.

```
admin@edge:~$ service webproxy restart
Restarting Squid HTTP proxy: squid .......done.
admin@edge:~$
```

25.4.91 service webproxy show blacklist categories

Показывает перечень категорий, доступ к которым нежелателен ("чёрный" список категорий).

Синтаксис

```
service webproxy show blacklist categories
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Указания по использованию

С помощью этой команды можно ознакомиться с перечнем известных на момент отдачи команды веб-прокси категорий адресов.

25.4.92 service show webproxy blacklist domains

Показывает перечень доменов, доступ к которым нежелателен ("чёрный" список доменов).

Синтаксис

```
service webproxy show blacklist domains [<категория>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

категория

Показать перечень доменов для определенной категории.

Указания по использованию

С помощью этой команды можно ознакомиться с перечнем всех известных на момент отдачи команды веб-прокси доменов из всех категорий.

25.4.93 service webproxy show blacklist log

Показывает протокол (журнал) запросов по адресам, находящимся в "чёрных" списках.

Синтаксис

```
show webproxy blacklist log [summary]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

summary

Вывести сводку по запросам к адресам, находящимся в "чёрных" списках.

Указания по использованию

Показать записанную в журнальный файл информацию о фактах обращения по адресам из "чёрных" списков вместе с адресом источника запроса.

25.4.94 service webproxy show blacklist search <текст>

Ищет в "чёрных" списках домены и/или адреса, включающие в себя указанный текст. IP-адреса в списках при этом тоже рассматриваются как текст.

Синтаксис

```
service webproxy show  blacklist search <текст>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

текст

Текст для поиска.

Указания по использованию

С помощью этой команды можно найти все записи во всех "чёрных" списках, включающие в себя указанный в команде текст.

25.4.95 service webproxy show blacklist urls

Показывает перечень URL, переход по которым нежелателен ("чёрный" список URL).

Синтаксис

```
service webproxy show blacklist urls [<категория>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

категория

Показать перечень URL для определенной категории.

Указания по использованию

С помощью этой команды можно ознакомиться с перечнем всех известных на момент отдачи команды веб-прокси URL из всех категорий.

25.4.96 service webproxy show log

Вывод на экран протокола (журнала) всех запросов пользователей к веб-прокси.

Синтаксис

```
service webproxy show log
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Указания по использованию

Эта команда выводит на экран содержимое файла-журнала, содержащего информацию о всех запросах, принятых веб-прокси.

26 Настройка RIP

26.1 Обзор RIP

Протокол RIP (Routing Information Protocol, протокол передачи маршрутной информации) – это протокол динамической маршрутизации, пригодный для небольших, однородных сетей. Он классифицируется как протокол внутренних шлюзов (IGP); в нем используется алгоритм маршрутизации типа «расстояние-направление». В RIP наилучший путь определяется путем подсчета транзитных узлов до получателя. Максимальное число транзитных узлов – 15 (16 считается бесконечным расстоянием), что делает RIP менее пригодным для больших сетей. Протокол RIP считается устаревшим и нежелательным для применения, вместо него рекомендуется использовать более новый протокол OSPF.

26.1.1 Поддерживаемые стандарты

Реализация протокола RIP соответствует следующим стандартам:

- RFC 1058: Routing Information Protocol.
- RFC 2453: RIP Version 2.

26.1.2 Настройка RIP

В этом разделе рассматриваются следующие вопросы:

- Основная настройка RIP
- Проверка настройки RIP

В данном разделе описан пример настройки для протокола RIP. Пример настройки основан на эталонной схеме, приведенной на рисунке.

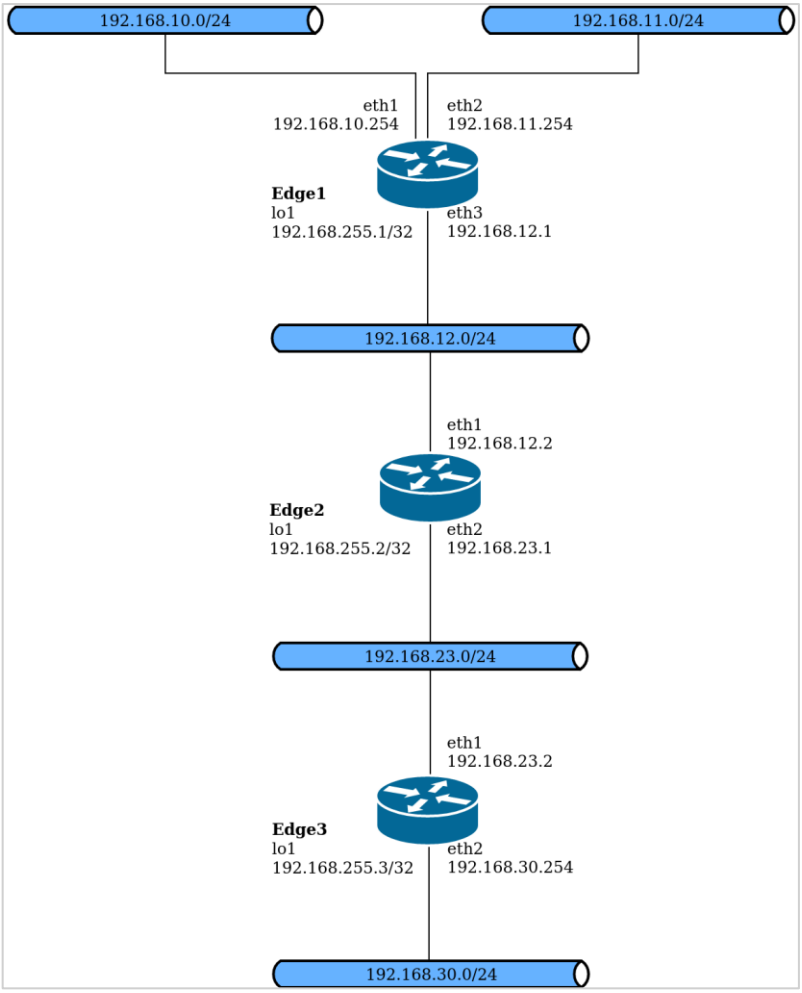


Рисунок 59 – Эталонная схема настройки RIP

26.1.3 Основная настройка RIP

В данном разделе выполняется настройка протокола RIP на маршрутизаторах, обозначенных на эталонной схеме как Edge1, Edge2 и Edge3. Эти маршрутизаторы объявляют свои маршруты в сетях 192.168.12.0/24 и 192.168.23.0/24.

В примере предполагается, что интерфейсы маршрутизаторов уже настроены; приведены только действия, необходимые для реализации RIP.

Для создания основной настройки RIP выполните следующие действия в режиме настройки:

Пример 233 – Основная настройка RIP

Маршрутизатор	**Действие**	**Команда**
Edge1	Объявление для сети 192.168.12.0/24.	`[edit]` `admin@Edge1# set protocols rip network 192.168.12.0/24`
Edge1	Перераспределение непосредственно подключенных маршрутов на RIP.	`[edit]` `admin@Edge1# set protocols rip redistribute connected`
Edge1	Фиксация настройки.	`[edit]` `admin@Edge1# commit`

Edge1	Отображение настройки.	`[edit]`
		`admin@Edge1# show protocols`
		`rip {`
		`network 192.168.12.0/24`
		`redistribute {`
		`connected {`
		`}`
		`}`
		`}`

Edge2	Объявление для сети 192.168.12.0/24.	`[edit]` `admin@Edge2# set protocols rip network 192.168.12.0/24`
Edge2	Объявление для сети 192.168.23.0/24.	`[edit]` `admin@Edge2# set protocols rip network 192.168.23.0/24`
Edge2	Перераспределение непосредственно подключенных маршрутов на RIP.	`[edit]` `admin@Edge2# set protocols rip redistribute connected`
Edge2	Фиксация настройки.	`[edit]` `admin@Edge2# commit`

Edge2	Отображение настройки.	`[edit]`
		`admin@Edge2# show protocols`
		`rip {`
		`network 192.168.12.0/24`
		`network 192.168.23.0/24`
		`redistribute {`
		`connected {`
		`}`
		`}`
		`}`

Edge3	Объявление для сети 192.168.23.0/24.	`[edit]` `admin@Edge3# set protocols rip network 192.168.23.0/24`
Edge3	Перераспределение непосредственно подключенных маршрутов на RIP.	`[edit]` `admin@Edge3# set protocols rip redistribute connected`
Edge3	Фиксация настройки.	`[edit]` `admin@Edge3# commit`
Edge3	Отображение настройки.	`[edit]` `admin@Edge3# show protocols`

Маршрутизатор	Действие	Команда

		rip {
		network 192.168.23.0/24
		redistribute {
		connected {
		}
		}
		}

26.1.4 Проверка настройки RIP

Для проверки настройки RIP можно использовать команды эксплуатационного режима.

В примере 234 приведен образец вывода команды **show ip route** для маршрутизатора Edge3.

Пример 234 – Проверка RIP на Edge3: «show ip route»

```
admin@Edge3:~$ show ip route

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I -
ISIS, B - BGP, > - selected route, * - FIB route

R>* 192.168.10.0/24 [120/3] via 192.168.23.1, eth1, 00:20:16

R>* 192.168.11.0/24 [120/3] via 192.168.23.1, eth1, 00:34:04

R>* 192.168.12.0/24 [120/2] via 192.168.23.1, eth1, 02:15:26

C>* 192.168.23.0/24 is directly connected, eth1

C>* 192.168.30.0/24 is directly connected, eth2

C>* 127.0.0.0/8 is directly connected, lo

admin@Edge3:~$
```

Также информацию о маршрутах можно получить с помощью команды **show ip rip.** В результате выполнения этой команды для Edge3 отображаются аналогичные сведения, но в другом формате, что представлено в примере ниже.

Пример 235 – Проверка RIP на Edge3: «show ip rip»

```
admin@Edge3:~$ show ip rip

Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP

Sub-codes:

            (n) - normal, (s) - static, (d) - default, (r) — redistribute,
            (i) - interface



            Network         Next Hop        Metric From   Tag      Time

R(n)     192.168.10.0/24    192.168.23.1         3          192.168.23.1
0          00:23

R(n)     192.168.11.0/24    192.168.23.1         3          192.168.23.1
0          00:23

R(n)     192.168.12.0/24    192.168.23.1         2          192.168.23.1
0          00:23

C(i)      192.168.23.0/24    0.0.0.0 1          self      0

C(r) 192.168.30.0/24        0.0.0.0 1 self (connected:1)    0
```

Из вывода видно, что маршруты к 192.168.10.0/24, 192.168.11.0/24 и 192.168.12.0/24 получены по RIP и что пакеты к этим сетям будут пересылаться наружу через интерфейс eth5 на 192.168.23.1. Сети 192.168.23.0/24 и 192.168.30.0/24 подключены непосредственно.

При помощи команды **ping** с маршрутизатора Edge3 можно убедиться, что узлы в удаленных сетях достижимы. В данном случае проверяется достижимость IP-адреса маршрутизатора Edge1. Результат показан в примере ниже.

Пример 236– Проверка RIP на Edge3: «ping 192.168.10.254»

```
admin@Edge3:~$ ping 192.168.10.254
PING 10.0.20.1 (10.0.20.1) 56(84) bytes of data.
64 bytes from 192.168.10.254: icmp_seq=1 ttl=63 time=8.63 ms
64 bytes from 192.168.10.254: icmp_seq=2 ttl=63 time=6.73 ms
64 bytes from 192.168.10.254: icmp_seq=3 ttl=63 time=8.77 ms
^C
-- 192.168.10.1 ping statistics --
3 packets transmitted, 3 received, 0% packet loss, time 2003ms rtt
min/avg/max/mdev = 6.739/8.048/8.775/0.927 ms
```

Тем самым получено подтверждение работоспособности настройки RIP и достижимости уделенной сети.

26.2 Команды настройки на уровне маршрутизатора

Команды настройки	
protocols rip default-distance <дистанция>	Установка административной дистанции для RIP.
protocols rip default-information originate	Создание маршрута по умолчанию в область маршрутизации RIP.
protocols rip default-metric <метрика>	Установка метрики по умолчанию для внешних маршрутов, перераспределенных на RIP.
protocols rip interface <интерфейс>	Включение протокола RIP на интерфейсе.
protocols rip neighbor <адрес>	Определение маршрутизатора, соседнего по RIP.
protocols rip network <подсеть>	Указание подсети для протокола RIP.

protocols rip network-distance <подсеть> [access-list <имя_списка> | distance <расстояние>]	Указание административного расстояния до подсети RIP.
protocols rip passive-interface <интерфейс>	Установка пассивного режима для указанного интерфейса.
protocols rip route <подсеть>	Указание статического маршрута RIP.
protocols rip timers garbage-collection <время>	Установка таймеров для сборки мусора RIP.
protocols rip timers timeout <время>	Установка интервала для времени неактивности RIP.
protocols rip timers update <время>	Установка таймера для обновления таблицы маршрутизации RIP.
Команды перераспределения маршрутов	
protocols rip redistribute bgp	Перераспределение маршрутов BGP в таблицы маршрутизации RIP.
protocols rip redistribute connected	Перераспределение непосредственно подключенных маршрутов в таблицы маршрутизации RIP.
protocols rip redistribute kernel	Перераспределение маршрутов ядра в таблицы маршрутизации RIP.
protocols rip redistribute ospf	Перераспределение маршрутов OSPF в таблицы маршрутизации RIP.
protocols rip redistribute static	Перераспределение статических маршрутов в таблицы маршрутизации RIP.
Команды фильтрации маршрутов	
protocols rip distribute-list access-list	Применение списка доступа к фильтрации входящих или исходящих пакетов RIP.
protocols rip distribute-list interface <интерфейс> access-list	Применение списка доступа к конкретному интерфейсу для фильтрации входящих или исходящих пакетов RIP.
protocols rip distribute-list interface <интерфейс> prefix-list	Применение списка префиксов к конкретному интерфейсу для фильтрации входящих или исходящих пакетов RIP.
protocols rip distribute-list prefix-list	Применение списка префиксов к фильтрации входящих или исходящих пакетов RIP.
Команды для интерфейсов	
interfaces <интерфейс> ip rip	Включение RIP на интерфейсе.
interfaces <интерфейс> ip rip authentication	Указание аутентификации RIP на интерфейсе.
interfaces <интерфейс> ip rip split-horizon	Настройка разделения горизонта в информации RIP, приходящей с указанного интерфейса.
Эксплуатационные команды	
routing rip debug enable events	Включение или отключение вывода отладочных сообщений, относящихся к событиям RIP.
routing rip debug enable packet	Включение или отключение вывода отладочных сообщений, относящихся ко всем типам пакетов RIP.
routing rip debug enable zebra	Включение или отключение вывода отладочных сообщений для процесса Zebra, работающего с протоколом RIP.
routing rip debug status	Отображение флагов отладки протокола RIP.
show ip route rip	Отображение всех маршрутов RIP по IP.
show ip rip	Отображение сведений о протоколе RIP.

26.2.1 protocols rip default-distance <дистанция>

Установка административной дистанции для RIP.

Синтаксис

```
set protocols rip default-distance <дистанция>
delete protocols rip default-distance
show protocols rip default-distance
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   rip {
      default-distance дистанция
   }
}
```

Параметры

дистанция

Обязательный. Установка административного расстояния по умолчанию для протокола RIP. Значение должно находиться в диапазоне от 1 до 255.

Значение по умолчанию

Административное расстояние по умолчанию для протокола RIP равно 120.

Указания по использованию

Форма **set** этой команды используется для установки административного расстояния по умолчанию для RIP.

Форма **delete** этой команды используется для восстановления административного расстояния по умолчанию для RIP.

Форма **show** этой команды используется для отображения административного расстояния по умолчанию для RIP.

26.2.2 protocols rip default-information originate

Создание маршрута по умолчанию в область маршрутизации RIP.

Синтаксис

```
set protocols rip default-information originate
delete protocols rip default-information originate
show protocols rip default-information
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   rip {
      default-information {
         originate
      }
   }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

По умолчанию система не создает внешний маршрут в область маршрутизации RIP.

Указания по использованию

Форма **set** этой команды используется для создания маршрута по умолчанию в область маршрутизации RIP.

Форма **delete** этой команды используется для восстановления поведения по умолчанию для создания маршрута по умолчанию в RIP.

Форма **show** этой команды используется для отображения настройки создания маршрута по умолчанию.

26.2.3 protocols rip default-metric <метрика>

Установка метрики по умолчанию для внешних маршрутов, перераспределенных на RIP.

Синтаксис

```
set protocols rip default-metric <метрика>
delete protocols rip default-metric
show protocols rip default-metric
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   rip {
      default-metric метрика
   }
}
```

Параметры

метрика

Обязательный. Метрика будет назначена внешним маршрутам, импортированным в RIP для перераспределения. Значение должно находиться в диапазоне от 1 до 16.

Значение по умолчанию

Маршрутам, импортируемым в RIP, назначается метрика 1.

Указания по использованию

Форма **set** этой команды используется для установки метрики для маршрутов, перераспределяемых в RIP.

Форма **delete** этой команды используется для восстановления значения по умолчанию для метрики RIP по умолчанию.

Форма **show** этой команды используется для отображения метрики по умолчанию для маршрутов, перераспределяемых на RIP.

26.2.4 protocols rip interface <интерфейс>

Включение протокола RIP на интерфейсе.

Синтаксис

```
set protocols rip interface <интерфейс>
delete protocols rip interface <интерфейс>
show protocols rip interface
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   rip {
      interface интерфейс
   }
```

```
}
```

Параметры

интерфейс

Обязательный. Множественный узел. Имя определенного интерфейса, на котором будет запущен RIP.

Можно включить RIP более чем на одном интерфейсе путем создания нескольких узлов конфигурации protocols rip interface.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для включения RIP на интерфейсе. Чтобы интерфейс можно было использовать для маршрутизации с помощью RIP, на интерфейсе должен быть включен протокол RIP.

Форма **delete** этой команды используется для отключения RIP на интерфейсе.

Форма **show** этой команды используется для отображения настройки протокола RIP на интерфейсе.

26.2.5 protocols rip neighbor <адрес>

Определение маршрутизатора, соседнего по RIP.

Синтаксис

```
set protocols rip neighbor <адрес>
delete protocols rip neighbor <адрес>
show protocols rip neighbor
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   rip {
      neighbor адрес
   }
}
```

Параметры

адрес

Обязательный. Множественный узел. IP-адрес соседнего маршрутизатора.

Можно определить более одного соседнего по RIP маршрутизатора путем создания нескольких узлов конфигурации protocols rip neighbor.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для определения соседнего по RIP маршрутизатора.

Форма **delete** этой команды используется для удаления соседнего маршрутизатора.

Форма **show** этой команды используется для отображения настройки соседей по RIP.

26.2.6 protocols rip network <подсеть>

Указание подсети для протокола RIP.

Синтаксис

```
set protocols rip network <подсеть>
```

```
delete protocols rip network <подсеть>
show protocols rip network
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    rip {
        network подсеть
    }
}
```

Параметры

подсеть

Обязательный. Множественный узел. Адрес подсети RIP в формате ip-адрес/маска.

Можно определить более одной сети RIP путем создания нескольких узлов конфигурации protocols rip network.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для указания подсети RIP.

Форма **delete** этой команды используется для удаления подсети RIP.

Форма **show** этой команды используется для отображения настройки подсети RIP.

26.2.7 protocols rip network-distance <подсеть> [access-list <имя_списка> | distance <расстояние>]

Указание административного расстояния до подсети RIP.

Синтаксис

```
set protocols rip network-distance <подсеть> [access-list <имя_списка> | distance <расстояние>]
delete protocols rip network-distance <подсеть> [access-list <имя_списка> | distance <расстояние>]
show protocols rip network-distance <подсеть> [access-list | distance]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    rip {
        network-distance подсеть {
            access-list имя_списка
            distance расстояние
        }
    }
}
```

Параметры

подсеть

Обязательный. Адрес в формате подсети IP, определяющий подсеть.

имя_списка

Имя списка доступа, применяемого к указанной подсети.

расстояние

Обязательный. Административное расстояние, применяемое к указанной подсети. Значение должно находиться в диапазоне от 1 до 255.

Значение по умолчанию

Отсутствует.

Указания по использованию

Административное расстояние отражает степень доверия к маршрутизатору или группе маршрутизаторов как к источнику маршрутной информации: чем больше значение, тем меньше степень доверия к элементу. Административное расстояние, равное 1, обычно означает непосредственно подключенную сеть, а равное 255 – неизвестный или ненадежный источник маршрутной информации. Обычно к RIP применяется административное расстояние 120.

Форма **set** этой команды используется для установки административного расстояния до подсети RIP или для применения списка доступа к подсети RIP.

Форма **delete** этой команды используется для восстановления административного расстояния по умолчанию до подсети RIP или для удаления списка доступа.

Форма **show** этой команды используется для отображения административного расстояния до подсети RIP или примененных списков доступа.

26.2.8 protocols rip passive-interface <интерфейс>

Установка пассивного режима для указанного интерфейса.

Синтаксис

```
set protocols rip passive-interface <интерфейс>
delete protocols rip passive-interface <интерфейс>
show protocols rip passive-interface
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   rip {
      passive-interface интерфейс
   }
}
```

Параметры

интерфейс

Обязательный. Множественный узел. Имя настроенного интерфейса, на котором следует установить пассивный режим.

Для того чтобы установить пассивный режим на нескольких интерфейсах, следует создать соответствующее число узлов конфигурации protocols rip passive-interface.

Значение по умолчанию

Пассивный режим не установлен.

Указания по использованию

Данная команда позволяет установить пассивный режим для указанного интерфейса. При использовании пассивного режима все получаемые пакеты RIP будут обработаны, но обновления будут отправляться только соседям, объявленным при помощи команды **protocols rip neighbor <ipv4-адрес>**.

Форма **set** используется установки пассивного режима на интерфейсе.

Форма **delete** этой команды используется для отмены пассивного режима на интерфейсе.

Форма **show** этой команды используется для отображения настройки пассивного режима на интерфейсе.

protocols rip route <подсеть>

Указание статического маршрута RIP.

Синтаксис

```
set protocols rip route <подсеть>
delete protocols rip route <подсеть>
show protocols rip route
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   rip {
      route подсеть
   }
}
```

Параметры

подсеть

Обязательный. Адрес подсети, определяющий статический маршрут RIP.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для определения статического маршрута RIP.

Форма **delete** этой команды используется для удаления статического маршрута RIP.

Форма **show** этой команды используется для отображения настройки статических маршрутов RIP.

26.2.9 protocols rip timers garbage-collection <время>

Установка таймеров для сборки мусора RIP.

Синтаксис

```
set protocols rip timers garbage-collection <время>
delete protocols rip timers garbage-collection <время>
show protocols rip timers garbage-collection
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   rip {
```

```
        timers {
            garbage-collection <время>
        }
    }
}
```

Параметры

время

Обязательный. Значение интервала таймера в секундах. Значение должно лежать в диапазоне от 5 до 2147483647.

Значение по умолчанию

Значение по умолчанию равно 120.

Указания по использованию

Форма **set** этой команды используется для установки таймера сборки мусора. Когда интервал таймера заканчивается, система выполняет поиск просроченных ресурсов RIP и освобождает их для использования.

Форма **delete** этой команды используется для восстановления значения по умолчанию таймера сборки мусора RIP.

Форма **show** этой команды используется для отображения настройки таймера сборки мусора RIP.

26.2.10 protocols rip timers timeout <время>

Установка интервала для времени неактивности RIP.

Синтаксис

```
set protocols rip timers timeout <время>
delete protocols rip timers timeout <время>
show protocols rip timers timeout
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    rip {
        timers {
            timeout время
        }
    }
}
```

Параметры

время

Обязательный. Интервал неактивности RIP в секундах. Значение должно лежать в диапазоне от 5 до 2147483647.

Значение по умолчанию

Состояние неактивности RIP возникает через 180 секунд.

Указания по использованию

Форма **set** этой команды используется для установки значения времени неактивности RIP.

Форма **delete** используется для сброса интервала неактивности RIP и восстановления значения по умолчанию.

Форма **show** этой команды используется для отображения настройки времени неактивности RIP.

26.2.11 protocols rip timers update <время>

Установка таймера для обновления таблицы маршрутизации RIP.

Синтаксис

```
set protocols rip timers update <время>
delete protocols rip timers update <время>
show protocols rip timers update
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   rip {
      timers {
         update время
      }
   }
}
```

Параметры

время

Обязательный. Интервал. с которым происходит обновление таблиц маршрутизации RIP. Значение должно лежать в диапазоне от 5 до 2147483647.

Значение по умолчанию

Таблица маршрутизации RIP обновляется каждые 30 секунд.

Указания по использованию

Форма **set** этой команды используется для установки интервала времени между обновлениями таблицы маршрутизации RIP. Чем короче интервал, тем более точна маршрутная информация в таблицах, но тем больше и трафик протокола через сеть.

Форма **delete** этой команды используется для восстановления значения интервала обновления RIP по умолчанию.

Форма **show** этой команды используется для отображения настройки интервала обновления RIP.

26.2.12 protocols rip redistribute bgp

Перераспределение маршрутов BGP в таблицы маршрутизации RIP.

Синтаксис

```
set protocols rip redistribute bgp [metric <метрика> | route-map <имя_карты>]
delete protocols rip redistribute bgp [metric | route-map]
show protocols rip redistribute bgp [metric | route-map]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   rip {
      redistribute {
```

```
            bgp {
               metric метрика
               route-map имя_карты
            }
         }
      }
   }
```

Параметры

метрика

Метрика маршрутизации для применения к маршрутам BGP, импортируемым в таблицы маршрутизации RIP. Значение должно лежать в диапазоне от 1 до 16.

имя_карты

Необязательный. Применение указанной карты маршрутов к маршрутам BGP, импортируемым в таблицы маршрутизации RIP.

Значение по умолчанию

Маршрутам BGP, перераспределяемым в RIP, назначается метрика маршрутизации 1. По умолчанию к перераспределяемым маршрутам BGP никакие карты маршрутов не применяются.

Указания по использованию

Форма **set** этой команды используется для установки метрики маршрутизации для маршрутов BGP, перераспределяемых в RIP, или для указания карты маршрутов, применяемой к перераспределяемым маршрутам BGP.

Форма **delete** этой команды используется для удаления настройки перераспределения маршрутов BGP.

Форма **show** этой команды используется для отображения настройки перераспределения маршрутов BGP.

26.2.13 protocols rip redistribute connected

Перераспределение непосредственно подключенных маршрутов в таблицы маршрутизации RIP.

Синтаксис

```
set protocols rip redistribute connected [metric <метрика> | route-map <карта_маршрутов>]
delete protocols rip redistribute connected [metric | route-map]
show protocols rip redistribute connected [metric | route-map]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   rip {
      redistribute {
         connected {
            metric метрика
            route-map имя_карты
         }
      }
   }
}
```

Параметры

метрика

Необязательный. Метрика маршрутизации для применения к непосредственно подключенным маршрутам, импортируемым в таблицы маршрутизации RIP. Значение должно лежать в диапазоне от 1 до 16.

имя_карты

Необязательный. Применение указанной карты маршрутов к непосредственно подключенным маршрутам, импортируемым в таблицы маршрутизации RIP.

Значение по умолчанию

Непосредственно подключенным маршрутам, перераспределяемым в RIP, назначается метрика маршрутизации 1. По умолчанию к перераспределяемым непосредственно подключенным маршрутам никакие карты маршрутов не применяются.

Указания по использованию

Форма **set** этой команды используется для установки метрики маршрутизации на непосредственно подключенных маршрутах, перераспределяемых на RIP, или для указания карты маршрутов, применяемой к перераспределяемым непосредственно подключенным маршрутам.

Форма **delete** этой команды используется для удаления настройки перераспределения непосредственно подключенных маршрутов.

Форма **show** этой команды используется для отображения настройки перераспределения непосредственно подключенных маршрутов.

26.2.14 protocols rip redistribute kernel

Перераспределение маршрутов ядра в таблицы маршрутизации RIP.

Синтаксис

```
set protocols rip redistribute kernel [metric <метрика> | route-map <имя_карты>]
delete protocols rip redistribute kernel [metric | route-map]
show protocols rip redistribute kernel [metric | route-map]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    rip {
        redistribute {
            kernel {
                metric метрика
                route-map имя_карты
            }
        }
    }
}
```

Параметры

метрика

Необязательный. Метрика маршрутизации для применения к маршрутам ядра, импортируемым в таблицы маршрутизации RIP. Значение должно лежать в диапазоне от 1 до 16.

имя_карты

Необязательный. Применение указанной карты маршрутов к маршрутам ядра, импортируемым в таблицы маршрутизации RIP.

Значение по умолчанию

Маршрутам ядра, перераспределяемым в RIP, назначается метрика маршрутизации 1. По умолчанию к перераспределяемым маршрутам ядра никакие карты маршрутов не применяются.

Указания по использованию

Форма **set** этой команды используется для установки метрики маршрутизации на маршрутах ядра, перераспределяемых на RIP, или для указания карты маршрутов, применяемой к перераспределяемым маршрутам ядра.

Форма **delete** этой команды используется для удаления настройки перераспределения маршрутов ядра.

Форма **show** этой команды используется для отображения настройки перераспределения маршрутов ядра.

26.2.15 protocols rip redistribute ospf

Перераспределение маршрутов OSPF в таблицы маршрутизации RIP.

Синтаксис

```
set protocols rip redistribute ospf [metric <метрика> | route-map <имя_карты>]

delete protocols rip redistribute ospf [metric | route-map]

show protocols rip redistribute ospf [metric | route-map]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    rip {
        redistribute {
            ospf {
                metric метрика
                route-map имя_карты
            }
        }
    }
}
```

Параметры

метрика

Необязательный. Метрика маршрутизации для применения к маршрутам OSPF, импортируемым в таблицы маршрутизации RIP. Значение должно лежать в диапазоне от 1 до 16.

имя_карты

Необязательный. Применение указанной карты маршрутов к маршрутам OSPF, импортируемым в таблицы маршрутизации RIP.

Значение по умолчанию

Маршрутам OSPF, перераспределяемым в RIP, назначается метрика маршрутизации 1. По умолчанию к перераспределяемым маршрутам OSPF никакие карты маршрутов не применяются.

Указания по использованию

Форма **set** этой команды используется для установки метрики маршрутизации на маршрутах OSPF, перераспределяемых на RIP, или для указания карты маршрутов, применяемой к перераспределяемым маршрутам OSPF.

Форма **delete** этой команды используется для удаления настройки перераспределения маршрутов OSPF.

Форма **show** этой команды используется для отображения настройки перераспределения маршрутов OSPF.

26.2.16 protocols rip redistribute static

Перераспределение статических маршрутов в таблицы маршрутизации RIP.

Синтаксис

```
set protocols rip redistribute static [metric <метрика> | route-map <имя_карты>]
delete protocols rip redistribute static [metric | route-map]
show protocols rip redistribute static [metric | route-map]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    rip {
        redistribute {
            static {
                metric метрика
                route-map имя_карты
            }
        }
    }
}
```

Параметры

метрика

Необязательный. Метрика маршрутизации для применения к статическим маршрутам, импортируемым в таблицы маршрутизации RIP. Значение должно лежать в диапазоне от 1 до 16.

имя_карты

Необязательный. Применение указанной карты маршрутов к статическим маршрутам, импортируемым в таблицы маршрутизации RIP.

Значение по умолчанию

Статическим маршрутам, перераспределяемым в RIP, назначается метрика маршрутизации 1. По умолчанию к перераспределяемым статическим маршрутам никакие карты маршрутов не применяются.

Указания по использованию

Форма **set** этой команды используется для установки метрики маршрутизации на статических маршрутах, перераспределяемых на RIP, или для указания карты маршрутов, применяемой к перераспределяемым статическим маршрутам.

Форма **delete** этой команды используется для удаления настройки перераспределения статических маршрутов.

Форма **show** этой команды используется для отображения настройки перераспределения статических маршрутов.

26.2.17 protocols rip distribute-list access-list

Применение списка доступа к фильтрации входящих или исходящих пакетов RIP.

Синтаксис

```
set protocols rip distribute-list access-list [in <список_доступа> | out <список_доступа>]

delete protocols rip distribute-list access-list [in | out]

show protocols rip distribute-list access-list [in | out]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   rip {
      distribute-list {
         access-list {
            in список_доступа
            out список_доступа
         }
      }
   }
}
```

Параметры

список_доступа

Идентификатор определенного списка доступа. Указанный список доступа будет применен для фильтрации пакетов RIP.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для применения списка доступа к фильтрации входящих или исходящих пакетов RIP.

Форма **delete** этой команды используется для удаления фильтрации пакетов с помощью списка доступа из пакетов RIP.

Форма **show** этой команды используется для отображения настройки фильтрации с помощью списков доступа в RIP.

26.2.18 protocols rip distribute-list interface <интерфейс> access-list

Применение списка доступа к конкретному интерфейсу для фильтрации входящих или исходящих пакетов RIP.

Синтаксис

```
set protocols rip distribute-list interface <интерфейс> access-list [in <список_доступа> | out <список_доступа>]

delete protocols rip distribute-list interface <интерфейс> access-list [in | out]

show protocols rip distribute-list interface <интерфейс> access-list [in | out]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   rip {
      distribute-list {
         interface интерфейс {
            access-list {
               in список_доступа
               out список_доступа
            }
         }
      }
   }
}
```

Параметры

интерфейс

Обязательный. Интерфейс, на котором будет выполняться фильтрация пакетов.

список_доступа

Идентификатор определенного списка доступа. Указанный список доступа будет применен для фильтрации пакетов RIP на указанном интерфейсе.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для применения списка доступа к фильтрации входящих или исходящих пакетов RIP на конкретном интерфейсе.

Форма **delete** этой команды используется для удаления фильтрации пакетов с помощью списка доступа в RIP с интерфейса.

Форма **show** этой команды используется для отображения настройки фильтрации с помощью списков доступа в RIP на интерфейсе.

26.2.19 protocols rip distribute-list interface <интерфейс> prefix-list

Применение списка префиксов к конкретному интерфейсу для фильтрации входящих или исходящих пакетов RIP.

Синтаксис

```
set protocols rip distribute-list interface <интерфейс> prefix-list [in <список_префиксов> | out <список_префиксов>]

delete protocols rip distribute-list interface <интерфейс> prefix-list [in | out]

show protocols rip distribute-list interface <интерфейс> prefix-list [in | out]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    rip {
        distribute-list {
            interface интерфейс {
                prefix-list {
                    in список_префиксов
                    out список_префиксов
                }
            }
        }
    }
}
```

Параметры

интерфейс

Обязательный. Интерфейс, к которому будет применен фильтр по списку префиксов.

список_префиксов

Идентификатор определенного списка префиксов. Указанный список префиксов будет применен для фильтрации пакетов RIP на указанном интерфейсе.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для применения списка префиксов к фильтрации входящих или исходящих пакетов RIP на конкретном интерфейсе.

Форма **delete** этой команды используется для удаления фильтрации пакетов с помощью списка префиксов в RIP с интерфейса.

Форма **show** этой команды используется для отображения настройки фильтрации с помощью списков префиксов в RIP на интерфейсе.

26.2.20 protocols rip distribute-list prefix-list

Применение списка префиксов к фильтрации входящих или исходящих пакетов RIP.

Синтаксис

```
set protocols rip distribute-list prefix-list [in  <список_префиксов> | out <список_префиксов>]

delete protocols rip distribute-list prefix-list [in | out]

show protocols rip distribute-list prefix-list [in | out]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    rip {
        distribute-list {
            prefix-list {
                in список_префиксов
```

```
                out список_префиксов
            }
        }
    }
}
```

Параметры

список_префиксов

Идентификатор определенного списка префиксов. Указанный список префиксов будет применен для фильтрации пакетов RIP.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для применения списка префиксов к фильтрации входящих или исходящих пакетов RIP.

Форма **delete** этой команды используется для удаления фильтрации пакетов с помощью списка префиксов в RIP.

Форма **show** этой команды используется для отображения настройки фильтрации с помощью списков префиксов в RIP.

26.2.21 interfaces <интерфейс> ip rip

Включение RIP на интерфейсе.

Синтаксис

```
set interfaces <интерфейс> ip rip
delete interfaces <интерфейс> ip rip
show interfaces <интерфейс> ip rip
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
    ip {
        rip
    }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса и конкретный интерфейс.

Значение по умолчанию

Отсутствует.

Указания по использованию

Это команда используется для включения протокола RIP на интерфейсе.

Форма **set** этой команды используется для включения RIP на интерфейсе.

Форма **delete** этой команды используется для удаления всей настройки RIP и отключения RIP на указанном интерфейсе.

Форма **show** этой команды используется для отображения настройки RIP.

26.2.22 interfaces <интерфейс> ip rip authentication

Указание аутентификации RIP на интерфейсе.

Синтаксис

```
set interfaces <интерфейс> ip rip authentication [md5 <номер_ключа> password <md5_ключ> | plaintext-password <пароль>]

delete interfaces <интерфейс> ip rip authentication [md5 | plaintext-password]

show interfaces <интерфейс> ip rip authentication [md5 | plaintext-password]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces <интерфейс> {
    ip {
        rip {
            authentication {
                md5 номер_ключа {
                    password md5_ключ
                }
                plaintext-password пароль
            }
        }
    }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса.

номер_ключа

Необязательный. Идентификатор ключа аутентификации. Он должен быть одинаковым на отправляющей и принимающей системах. Значение должно находиться в диапазоне от 1 до 255.

md5_ключ

Необязательный. Пароль, используемый в аутентификации MD5. Он должен быть одинаковым на отправляющей и принимающей системах.

пароль

Необязательный. Пароль, используемый в простой аутентификации (открытыми текстом). Он должен быть одинаковым на отправляющей и принимающей системах.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания метода аутентификации, используемого протоколом RIP на интерфейсе. Указанный метод независим от аутентификации, настроенной в области RIP.

При простой аутентификации пароли передаются через сеть открытым текстом (в незашифрованном виде). При аутентификации MD5 в системе используется алгоритм Message Digest 5 (MD5) для вычисления значения хеш-кода из содержимого пакета и пароля RIP. Вычисленное значение хеш-кода и ключ MD5 включаются в

состав передаваемого пакета, и принимающая система (настроенная с тем же самым паролем) вычисляет свой хеш-код, который должен соответствовать передаваемому.

Параметры аутентификации должны быть одинаковыми на всех маршрутизаторах, предназначенных для установления двунаправленной связи в сети. Если параметры аутентификации на двух маршрутизаторах не согласованы, их соседство не будет установлено, и каждый из них не будет учитывать связи, устанавливаемые на другом.

Форма **set** этой команды используется для установки аутентификации RIP на интерфейсе.

Форма **delete** этой команды используется для удаления сведений о настройке аутентификации RIP на интерфейсе.

Форма **show** этой команды используется для отображения сведений о настройке аутентификации RIP на интерфейсе.

26.2.23 interfaces <интерфейс> ip rip split-horizon

Настройка разделения горизонта в информации RIP, приходящей с указанного интерфейса.

Синтаксис

```
set interfaces <интерфейс> ip rip split-horizon [disable | poison-reverse]
delete interfaces <интерфейс> ip rip split-horizon [disable | poison-reverse]
show interfaces <интерфейс> ip rip split-horizon
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
   ip {
      rip {
        split-horizon {
           disable
           poison-reverse
        }
      }
   }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса.

disable

Отключение разделения горизонта на интерфейсе.

poison-reverse

Включение возврата заблокированных маршрутов на интерфейсе.

Значение по умолчанию

Разделение горизонта включено.

Указания по использованию

Эта команда используется для отключения разделения горизонта или для включения возврата заблокированных маршрутов при разделении горизонта на интерфейсе с работающим протоколом RIP.

Разделение горизонта – это функция, предназначенная для повышения стабильности и предотвращающая появление циклов в сети, особенно в случае обрыва каналов. Она останавливает включение в маршрутную

информацию интерфейса всех маршрутов, полученных с этого интерфейса. Разделение горизонта полезно при предотвращении циклов между маршрутизаторами, непосредственно подключенными друг к другу; оно ускоряет стабилизацию маршрутной информации при изменении условий в сети и включено по умолчанию в RIP.

Возврат заблокированных маршрутов является разновидностью разделения горизонта. Интерфейс с функцией возврата заблокированных маршрутов не останавливает отправку маршрута на маршрутизатор, с которого он был получен, но увеличивает метрику для него до 16 и рассылает эти сведения в следующей порции маршрутной информации. Так как в сети с протоколом RIP максимальное число транзитных узлов для маршрута, считающегося достижимым, составляет 15, то при увеличении метрики до 16 маршрут рассматривается как недостижимый. Это называется блокировкой маршрута. Возврат заблокированных маршрутов полезен для распространения сведений о некорректных маршрутах на маршрутизаторы, которые работают с сетью нижнего уровня, но не являются непосредственными соседями; в этой ситуации разделение горизонта неэффективно.

Когда режим возврата заблокированных маршрутов включен, маршрутизатор включает маршрут в объявления для соседа, от которого маршрут был получен. Когда этот режим выключен, маршрутизатор не включает маршрут в объявления для соседа, от которого маршрут был получен.

Форма **set** этой команды используется для настройки разделения горизонта и возврата заблокированных маршрутов при разделении горизонта на интерфейсе, на котором работает протокол RIP.

Форма **delete** этой команды используется для восстановления настройки по умолчанию.

Форма **show** этой команды используется для отображения настройки разделения горизонта.

26.2.24 routing rip debug enable events

Включение или отключение вывода отладочных сообщений, относящихся к событиям RIP.

Синтаксис

```
routing rip debug enable events
routing rip debug disable events
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для включения вывода сообщений уровня *trace*, относящихся к событиям протокола RIP.

Форма **disable** этой команды используется для отключения вывода отладочных сообщений для событий RIP.

26.2.25 routing rip debug enable packet

Включение или отключение вывода отладочных сообщений, относящихся ко всем типам пакетов RIP.

Синтаксис

```
routing rip debug enable packet [all | recv [detail] | send [detail]]
routing rip debug disable packet [all | recv | send ]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

all

Необязательный. Вывод отладочных данных для всех пакетов.

recv

Необязательный. Вывод отладочных данных для всех принятых пакетов.

send

Необязательный. Вывод отладочных данных для всех отправленных пакетов.

detail

Необязательный. Вывод подробных отладочных данных.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для включения вывода сообщений уровня *trace*, относящихся ко всем типам пакетов протокола RIP.

Форма **disable** этой команды используется для отключения вывода отладочных сообщений, относящихся ко всем типам пакетов протокола RIP.

26.2.26 routing rip debug enable zebra

Включение или отключение вывода отладочных сообщений для процесса Zebra, работающего с протоколом RIP.

Синтаксис

```
routing rip debug enable zebra
routing rip debug disable zebra
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Выводятся отладочные сообщения для действий, относящихся к процессу Zebra, работающему с протоколом RIP.

Указания по использованию

Эта команда используется для включения вывода сообщений уровня *trace*, относящихся к процессу Zebra, работающему с протоколом RIP.

Форма **disable** этой команды используется для отключения вывода отладочных сообщений, относящихся к процессу Zebra, работающему с протоколом RIP.

26.2.27 routing rip debug status

Отображение флагов отладки протокола RIP.

Синтаксис

```
routing rip debug status
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует

Указания по использованию

Эта команда используется для вывода режима отладки RIP.

26.2.28 show ip route rip

Отображение всех маршрутов RIP по IP.

Синтаксис

```
show ip route rip
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения маршрутов RIP, содержащихся в таблице RIB (Routing Information Base, база маршрутной информации).

Примеры

В примере приведен образец вывода всех маршрутов RIP из таблицы RIB.

Пример 237 – «show ip route rip»: отображение маршрутов

```
admin@edge# run show ip route rip

Codes: K - kernel route, C - connected, S - static, R - RIP,

       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,

       > - selected route, * - FIB route

R>* 10.150.150.0/24 [120/2] via 192.168.0.1, eth1, 00:06:46

R>* 192.168.23.0/24 [120/2] via 192.168.0.1, eth1, 00:06:46

R>* 192.168.30.0/24 [120/3] via 192.168.0.1, eth1, 00:06:00
```

26.2.29 show ip rip

Отображение сведений о протоколе RIP.

Синтаксис

```
show ip rip [status]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

status

Необязательный. Отображение сведений только о состоянии протокола RIP.

Значение по умолчанию

Отображение всех сведений протокола RIP.

Указания по использованию

Эта команда используется для просмотра сведений о протоколе RIP.

Примеры

В примере ниже приведен образец вывода сведений о протоколе RIP.

Пример 238 – «show ip rip»: отображение сведений RIP

```
admin@edge# run show ip rip
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
      (n) - normal, (s) - static, (d) - default, (r) - redistribute,
      (i) - interface

     Network            Next Hop         Metric From            Tag Time
R(n) 10.150.150.0/24    192.168.0.1           2 192.168.0.1       0 02:59
C(r) 192.168.0.0/24     0.0.0.0               1 self              0
C(r) 192.168.10.0/24    0.0.0.0               1 self              0
C(r) 192.168.11.0/24    0.0.0.0               1 self              0
C(i) 192.168.12.0/24    0.0.0.0               1 self              0
R(n) 192.168.23.0/24    192.168.0.1           2 192.168.0.1       0 02:59
R(n) 192.168.30.0/24    192.168.0.1           3 192.168.0.1       0 02:59
```

В примере ниже приведен образец вывода сведений о состоянии протокола RIP.

Пример 239 – «show ip rip status»: отображение сведений RIP

```
admin@edge# run show ip rip status
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 20 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing: connected
  Default version control: send version 2, receive any version
    Interface        Send  Recv   Key-chain
    eth1             2     1 2
  Routing for Networks:
    192.168.12.0/24
  Routing Information Sources:
    Gateway          BadPackets BadRoutes  Distance Last Update
    192.168.0.1              0         0       120   00:00:30
    192.168.12.2             0         0       120   00:00:30
  Distance: (default is 120)
```

27 Настройка OSFP

27.1 OSPF и туннельные интерфейсы

27.1.1 Обзор OSPF

Протокол OSPF (Open Shortest Path First, открытый протокол с выбором кратчайшего пути первым) - протокол динамической маршрутизации, в котором используется алгоритм состояния канала (Дейкстра) в противоположность протоколам (наподобие RIP), в которых используется алгоритм вектора расстояний. OSPF является протоколом внутренних шлюзов (IGP) и действует в одной автономной системе (AS). В протоколе OSPF каждый маршрутизатор объявляет состояние его собственных каналов (или подключений) в объявлении состояния каналов (link state advertisement, LSA), которое отправляется многоадресной рассылкой на другие маршрутизаторы в сети. Кроме того, каждый маршрутизатор использует объявления LSA, получаемые с других маршрутизаторов, для построения графа, представляющего топологию сети. При построении таблицы маршрутизации маршрутизатор применяет алгоритм выбора кратчайшего пути Дейкстры для поиска наилучшего пути к каждому узлу топологии сети через граф. Основой таблицы маршрутизации становится "дерево кратчайших путей". Протокол OSPF является иерархическим. В OSPF сеть разбивается на "области". Внутри каждой области на маршрутизаторах имеется только локальная маршрутная информация. Маршрутная информация о других областях вычисляется при помощи сводок путей, которыми обмениваются области. Это позволяет сократить объем сведений о топологии сети, которые маршрутизаторам приходится создавать и поддерживать, что делает OSPF неплохо подходящим для средних и более крупных сетей.

Реализация протокола OSPF соответствует стандарту RFC 2328: OSPF Version 2.

27.1.2 Взаимодействие с туннельными интерфейсами

Существуют некоторые нюансы взаимодействия протокола OSPF с туннельными интерфейсами и, в частности, с интерфейсом OpenVPN. Особенность туннельных интерфейсов заключается в том, что по умолчанию их типом является point-to-point. Поэтому, если мы имеем интерфейс OpenVPN, настроенный в режиме сервера, корректной работы может не получиться, так как тип point-to-point имеет очень жесткую семантику по RFC 2328 и подразумевает возможность установления только одного соседства, а режим сервера автоматически подразумевает под собой установление множества связей, т.е., установление типа point-to-multipoint. В то же время, в RFC 2328 тип point-to-multipoint определяется как множество связей типа point-to-point. В Numa edge тип подсети на интерфейсе настраивается с помощью команды **set interfaces <интерфейс> ip ospf network <тип>**. Таким образом, для корректной работы OSPF с OpenVPN, необходимо указывать тип point-to-multipoint как для интерфейса, настроенного в режиме сервера, так и для интерфейса, находящегося в режиме клиента при осуществлении нескольких соединений у соответствующего сервера.

27.2 Настройка OSPF

В данном разделе описан пример настройки для протокола OSPF. Пример настройки основан на эталонной схеме, приведенной на рисунке ниже.

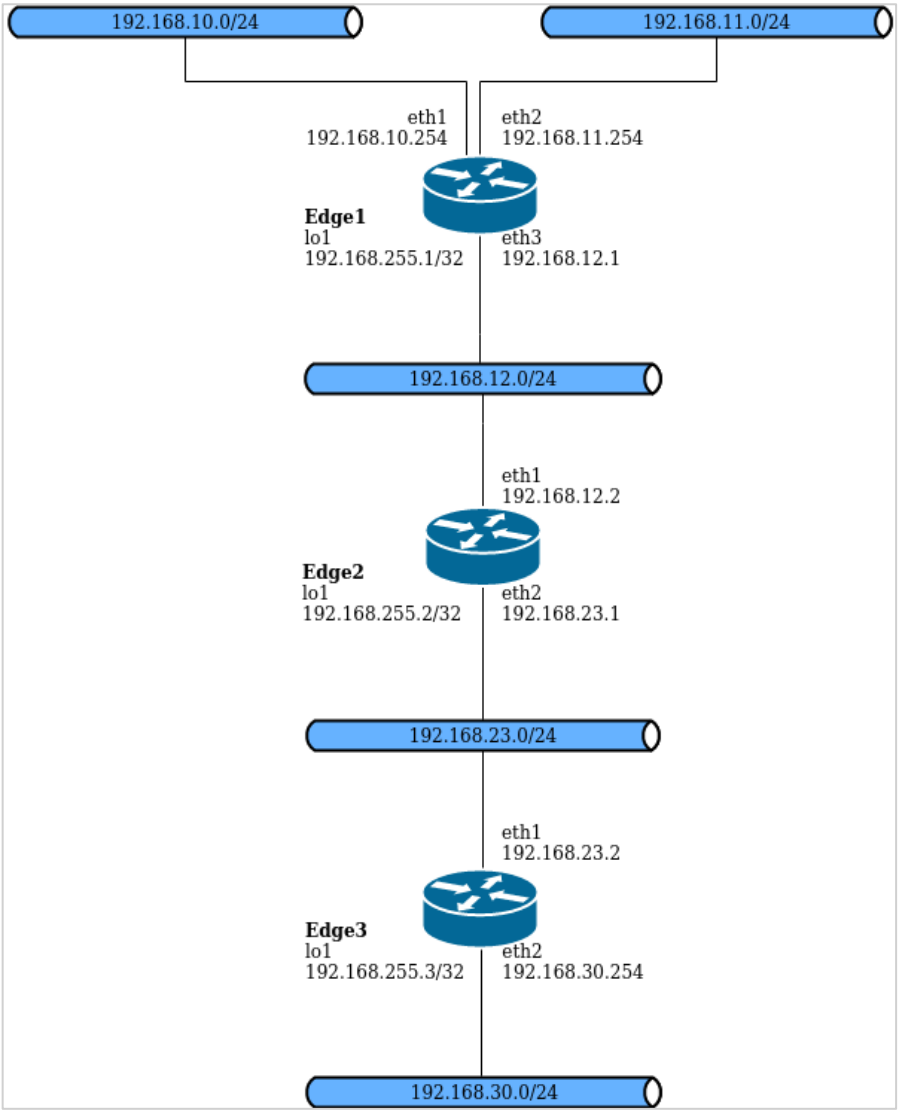


Рисунок 60 – Эталонная схема настройки OSPF

27.2.1 Проверка настройки OSPF

Для проверки настройки OSPF можно использовать ряд команд эксплуатационного режима.

show ip route

В примере ниже приведен вывод для команды **show ip route** для маршрутизатора Edge3.

Пример 240 – Проверка OSPF на Edge3: «show ip route»

```
admin@Edge3:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I -
ISIS, B - BGP, > - selected route, * - FIB route

O>* 192.168.255.1/32 [110/20] via 192.168.23.1, eth1, 00:04:21
O>* 192.168.255.2/32 [110/20] via 192.168.23.1, eth1, 00:03:31
C>* 192.168.255.3/32 is directly connected, lo
O>* 192.168.10.0/24 [110/20] via 192.168.23.1, eth1, 03:06:06
O>* 192.168.11.0/24 [110/20] via 192.168.23.1, eth1, 03:07:39
O>* 192.168.12.0/24 [110/20] via 192.168.23.1, eth1, 03:07:40
O 192.168.23.0/24 [110/10] is directly connected, eth1, 03:07:45
C>* 192.168.23.0/24 is directly connected, eth1
C>* 192.168.30.0/24 is directly connected, eth2
C>* 127.0.0.0/8 is directly connected, lo
```

Из вывода видно, что маршруты к 192.168.255.1/32, 192.168.255.2/32, 192.168.10.0/24, 192.168.11.0/24 и 192.168.12.0/24 получены по OSPF (и являются выбранными маршрутами). Кроме того, пакеты к этим сетям будут пересылаться наружу через eth1 на 192.168.23.1. 192.168.255.3/32, 192.168.23.0/24 и 192.168.30.0/24 подключены напрямую к Edge3. Непосредственно подключенные маршруты выбираются раньше любых обнаруженных с помощью OSPF (т.е. 192.168.23.0/24).

ping

При помощи команды **ping** с маршрутизатора Edge3 можно убедиться, что узлы в удаленных сетях достижимы. В примере проверяется достижимость IP-адреса Edge1.

Пример 241 – Проверка OSPF на Edge3: «ping 192.168.10.254»

```
admin@Edge3:~$ ping 192.168.10.254
PING 192.168.10.254 (192.168.10.254) 56(84) bytes of data.
64 bytes from 192.168.10.254: icmp_seq=1 ttl=63 time=5.75 ms
64 bytes from 192.168.10.254: icmp_seq=2 ttl=63 time=1.74 ms
64 bytes from 192.168.10.254: icmp_seq=3 ttl=63 time=1.40 ms
^C
– 192.168.10.254 ping statistics –
3 packets transmitted, 3 received, 0% packet loss, time 2002ms rtt
min/avg/max/mdev = 1.405/2.966/5.751/1.974 ms
```

Тем самым получено подтверждение работоспособности настройки OSPF и достижимости уделенной сети.

27.2.2 Основная настройка OSPF

В данном разделе выполняется настройка протокола OSPF на маршрутизаторах, обозначенных на эталонной схеме как Edge1, Edge2 и Edge3. Это маршрутизаторы объявляют свои маршруты в сетях 192.168.12.0/24 и 192.168.23.0/24.

В примере предполагается, что интерфейсы маршрутизаторов (в том числе интерфейсы заглушки lo) уже настроены; приведены только действия, необходимые для реализации OSPF.

Для создания основной настройки OSPF выполните следующие действия в режиме настройки:

Пример 242 – Основная настройка OSFP

Маршрутизатор	**Действие**	**Команда**
Edge1	Установка адреса интерфейса заглушки в качестве идентификатора маршрутизатора в OSPF.	`[edit]` `admin@Edge1# set protocols ospf parameters router-id 192.168.255.1`
Edge1	Объявление в сети 192.168.12.0/24.	`[edit]` `admin@Edge1# set protocols ospf area 0.0.0.0 network 192.168.12.0/24`
Edge1	Перераспределение непосредственно подключенных маршрутов на OSPF	`[edit]` `admin@Edge1# set protocols ospf redistribute connected`
Edge1	Фиксация настройки.	`[edit]` `admin@Edge1# commit`

Edge1	Отображение настройки.	`[edit]`
		`admin@Edge1# show protocols`
		`ospf {`
		`area 0.0.0.0 {`
		`network 192.168.12.0/24`
		`}`
		`parameters {`
		`router-id 192.168.255.1`
		`}`
		`redistribute {`
		`connected {`
		`}`
		`}`

Маршрутизатор	Действие	Команда
		} }
Edge2	Установка адреса интерфейса заглушки в качестве идентификатора маршрутизатора в OSPF.	[edit] admin@Edge2# set protocols ospf parameters router-id 192.168.255.2
Edge2	Объявление в сети 192.168.12.0/24.	[edit] admin@Edge2# set protocols ospf area 0.0.0.0 network 192.168.12.0/24
Edge2	Объявление для сети 192.168.23.0/24.	[edit] admin@Edge2# set protocols ospf area 0.0.0.0 network 192.168.23.0/24
Edge2	Перераспределение непосредственно подключенных маршрутов на OSPF	[edit] admin@Edge2# set protocols ospf redistribute connected
Edge2	Фиксация настройки.	[edit] admin@Edge2# commit

Edge2	Отображение настройки.	[edit]
		admin@Edge2# show protocols
		ospf {
		area 0.0.0.0 {
		network 192.168.12.0/24
		network 192.168.23.0/24
		}
		parameters {
		router-id 192.168.255.2
		}
		redistribute {
		connected {
		}
		}
		}

Edge3	Установка адреса интерфейса заглушки в качестве идентификатора маршрутизатора в OSPF.	[edit] admin@Edge3# set protocols ospf parameters router-id 192.168.255.3
Edge3	Объявление для сети 192.168.23.0/24.	[edit] admin@Edge3# set protocols ospf area 0.0.0.0 network 192.168.23.0/24
Edge3	Перераспределение непосредственно подключенных маршрутов на OSPF	[edit] admin@Edge3# set protocols ospf redistribute connected
Edge3	Фиксация настройки.	[edit] admin@Edge3# commit

Edge3	Отображение настройки.	[edit]
		admin@Edge3# show protocols
		ospf {
		area 0.0.0.0 {
		network 192.168.23.0/24
		}
		parameters {
		router-id 192.168.255.3
		}
		redistribute {
		connected {
		}
		}
		}

27.3 Команды настройки OSPF на уровне маршрутизатора

Команды настройки	
protocols ospf	Включение протокола маршрутизации OSPF на маршрутизаторе.
protocols ospf access-list <номер_списка>	Указание списка доступа для фильтрации сетей в маршрутной информации.
protocols ospf auto-cost reference-bandwidth <проп_спос>	Выдача системе директивы использовать метод эталонной пропускной способности для вычисления административной стоимости.
protocols ospf default-information originate	Установка характеристик внешнего маршрута по умолчанию, созданного в области маршрутизации OSPF.
protocols ospf default-metric <метрика>	Установка метрики по умолчанию, применяемой к маршрутам, перераспределяемым на OSPF.
protocols ospf distance	Установка административного расстояния OSPF по типу маршрута.
protocols ospf log-adjacency-changes	Включение или отключение протоколирования изменений в состоянии смежности для соседей.
protocols ospf max-metric router-lsa	Включение или отключение объявления максимального значения метрики на тупиковом маршрутизаторе OSPF при запуске или перезагрузке маршрутизатора.
protocols ospf mpls-te	Установка параметров управления направлением прохождения трафика при многопротокольной коммутации меток (MPLS-TE).
protocols ospf neighbor <ipv4-адрес>	Определение соседа по OSPF.
protocols ospf parameters	Установка глобальных параметров OSPF, таких как идентификатор маршрутизатора.
protocols ospf passive-interface <ethx>	Подавление маршрутной информации на интерфейсе.
protocols ospf refresh timers <время>	Установка значений для таймеров обновления OSPF.
protocols ospf timers throttle spf	Включение или отключение задержки вычислений SPF в OSPF.
Команды перераспределения маршрутов OSPF	
protocols ospf redistribute bgp	Установка параметров перераспределения маршрутов BGP на OSPF.
protocols ospf redistribute connected	Установка параметров перераспределения непосредственно подключенных маршрутов на OSPF.
protocols ospf redistribute kernel	Установка параметров перераспределения маршрутов ядра на OSPF.
protocols ospf redistribute rip	Установка параметров перераспределения маршрутов RIP на OSPF.
protocols ospf redistribute static	Установка параметров перераспределения статических маршрутов на OSPF.
Эксплуатационные команды	
routing ospf debug enable event	Включение или отключение вывода отладочных сообщений, относящихся к событиям OSPF.
routing ospf debug enable ism	Включение или отключение вывода отладочных сообщений, относящихся к ISM в OSPF.
routing ospf debug enable lsa	Включение или отключение вывода отладочных сообщений, относящихся к объявлениям состояния канала (LSA) в OSPF.
routing ospf debug enable ospf nsm	Включение или отключение вывода отладочных сообщений, относящихся к NSM в OSPF.
routing ospf debug enable nssa	Включение и отключение вывода отладочных сообщений, относящихся к малотупиковым областям (not-so-stubby areas, NSSA) в OSPF.
routing ospf debug enable packet all	Включение или отключение вывода отладочных сообщений, относящихся ко всем типам пакетов OSPF.
routing ospf debug enable packet dd	Включение или отключение вывода отладочных сообщений, относящихся к пакетам описания базы данных (DD) протокола OSPF.

routing ospf debug enable packet hello	Включение или отключение вывода отладочных сообщений, относящихся к пакетам приветствия протокола OSPF.
routing ospf debug enable packet ls-ack	Включение или отключение вывода отладочных сообщений, относящихся к пакетам уведомления о состоянии канала (LS Ack) протокола OSPF.
routing ospf debug enable packet ls-request	Включение или отключение вывода отладочных сообщений, относящихся к пакетам запроса состояния канала (LSR) протокола OSPF.
routing ospf debug enable packet ls-update	Включение или отключение вывода отладочных сообщений для пакетов обновления информации о состоянии канала (LSU) протокола OSPF.
routing ospf debug enable zebra	Включение или отключение вывода отладочных сообщений для процесса Zebra, работающего с протоколом OSPF.
routing osfp debug status	Отображение флагов отладки протокола OSPF.
show ip ospf	Отображение высокоуровневых сведений о настройке OSPF.
show ip ospf border-routers	Отображение сведений о граничных маршрутизаторах OSPF.
show ip ospf database	Отображение сведений о базе данных OSPF.
show ip ospf interface	Отображение сведений о настройке и состоянии OSPF для указанного интерфейса.
show ip ospf neighbor	Отображение сведений о соседях по OSPF для указанного адреса или интерфейса.
show ip ospf route	Отображение сведений о маршрутах OSPF.
show ip route ospf	Отображение всех маршрутов OSPF для IP.

27.3.1 protocols ospf

Включение протокола маршрутизации OSPF на маршрутизаторе.

Синтаксис

```
set protocols ospf
delete protocols ospf
show protocols ospf
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   ospf
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для включения протокола маршрутизации OSPF в системе.

Форма **set** этой команды используется для включения протокола маршрутизации OSPF.

Форма **delete** этой команды используется для отключения OSPF и удаления всей настройки OSPF.

Форма **show** этой команды используется для отображения настройки OSPF.

27.3.2 protocols ospf access-list <номер_списка>

Указание списка доступа для фильтрации сетей в маршрутной информации.

Синтаксис

```
set protocols ospf access-list <номер_списка> [export <тип>]
```

```
delete protocols ospf access-list <номер_списка> [export <тип>]
show protocols ospf access-list <номер_списка>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    ospf {
        access-list номер_списка {
            export тип      }
    }
}
```

Параметры

номер_списка

Обязательный. Номер списка доступа для фильтрации подсетей в маршрутной информации.

тип

Необязательный. Тип фильтруемых маршрутов. Список возможных значений: bgp, connected, kernel, rip, static. Можно указать несколько типов, создав дополнительные узлы настройки export.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания списка доступа, используемого при фильтрации подсетей в маршрутной информации.

Форма **set** этой команды используется для указания списка доступа.

Форма **delete** этой команды используется для удаления списка доступа.

Форма **show** этой команды используется для отображения настройки.

27.3.3 protocols ospf auto-cost reference-bandwidth <проп_спос>

Выдача системе директивы использовать метод эталонной пропускной способности для вычисления административной стоимости.

Синтаксис

```
set protocols ospf auto-cost reference-bandwidth <проп_спос>
delete protocols ospf auto-cost reference-bandwidth
show protocols ospf auto-cost reference-bandwidth
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    ospf {
        auto-cost {
            reference-bandwidth проп_спос
        }
    }
}
```

Параметры

проп_спос

Обязательный. Эталонная пропускная способность в мегабитах в секунду. Значение должно лежать в диапазоне от 1 до 4294967.

Значение по умолчанию

Эталонная пропускная способность по умолчанию равна 108.

Указания по использованию

Эта команда используется для установки эталонной пропускной способности, используемой при расчете стоимости OSPF. Метрика OSPF вычисляется как частное от деления эталонной пропускной способности на реальную пропускную способность. Автоматически вычисленные значения переопределяются явно установленной стоимостью для области.

Форма **set** этой команды используется для установки эталонной пропускной способности.

Форма **delete** этой команды используется для восстановления пропускной способности по умолчанию.

Форма **show** этой команды используется для отображения настройки автоматического расчета стоимости для OSPF.

27.3.4 protocols ospf default-information originate

Установка характеристик внешнего маршрута по умолчанию, созданного в области маршрутизации OSPF.

Синтаксис

```
set protocols ospf default-information originate [always | metric <метрика> | metric-type <тип> | route-map <имя_карты>]

delete protocols ospf default-information originate [always | metric | metric-type | route-map]

show protocols ospf default-information originate [always | metric | metric-type | route-map]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    ospf {
        default-information {
            originate {
                always
                metric метрика
                metric-type тип
                route-map имя_карты
            }
        }
    }
}
```

Параметры

always

Необязательный. Маршрут по умолчанию объявляется всегда.

метрика

Необязательный. Метрика, применяемая к маршруту по умолчанию. Значение должно лежать в диапазоне от 0 до 16777214. Значение по умолчанию равно 1.

тип

Необязательный. Тип метрики внешнего маршрута, связываемый с объявлением состояния канала (LSA). Поддерживаются следующие значения:

1: Внешний маршрут типа 1.

2: Внешний маршрут типа 2.

имя_карты

Необязательный. Если указанная карта маршрутов удовлетворяется, то создается маршрут по умолчанию.

Значение по умолчанию

По умолчанию система не создает внешний маршрут по умолчанию в область маршрутизации OSPF. Если такое создание разрешено, то умолчания зависят от типа области, в которой объявляется маршрут по умолчанию:

- в тупиковых областях создается объявление LSA типа 3 с метрикой, равной 1, а тип метрики игнорируется;
- в малотупиковых областях (NSSA), настроенных на импорт объявлений-сводок, создается объявление LSA типа 7 с метрикой, равной 1, и создается тип метрики 2;
- в областях NSSA, настроенных на отказ от импорта объявлений-сводок, создается объявление LSA типа 3 с метрикой, равной 1, а тип метрики игнорируется.

Указания по использованию

Эта команда используется для перераспределения маршрута по умолчанию (0.0.0.0) в область маршрутизации OSPF.

При таком перераспределении маршрутизатор автоматически становится граничным маршрутизатором автономной системы (Autonomous System Boundary Router, ASBR). Если не указано ключевое слово always, то для того, чтобы маршрутизатор смог создать маршрут по умолчанию, на нем уже должен быть настроен такой маршрут.

Форма **set** этой команды используется для включения создания внешнего маршрута по умолчанию в область маршрутизации OSPF.

Форма **delete** этой команды используется для включения создания внешнего маршрута по умолчанию в область маршрутизации OSPF или для восстановления значений параметров по умолчанию.

Форма **show** этой команды используется для отображения настройки распределения маршрутов по умолчанию.

27.3.5 protocols ospf default-metric <метрика>

Установка метрики по умолчанию, применяемой к маршрутам, перераспределяемым на OSPF.

Синтаксис

```
set protocols ospf default-metric <метрика>

delete protocols ospf default-metric

show protocols ospf default-metric
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   ospf {
      default-metric метрика
   }
}
```

Параметры

метрика

Обязательный. Метрика для применения к маршрутам из других протоколов, перераспределяемым на OSPF. Значение должно лежать в диапазоне от 0 до 16777214.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки метрики по умолчанию, применяемой к маршрутам из других протоколов, перераспределяемым на OSPF.

Форма **set** этой команды используется для установки метрики OSPF по умолчанию.

Форма **delete** этой команды используется для восстановления значения по умолчанию для метрики по умолчанию.

Форма **show** этой команды используется для отображения настройки метрики OSPF по умолчанию.

27.3.6 protocols ospf distance

Установка административного расстояния OSPF по типу маршрута.

Синтаксис

```
set protocols ospf distance [global <расстояние> | ospf [external <расстояние> | inter-area <расстояние> | intra-area <расстояние>]]

delete protocols ospf distance [global | ospf [external | inter-area | intra-area]]

show protocols ospf distance [global | ospf [external | inter-area | intra-area]]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    ospf {
        distance {
            global расстояние
            ospf {
                external 1-255
                inter-area 1-255
                intra-area 1-255
            }
        }
    }
}
```

Параметры

global *расстояние*

Административное расстояние, устанавливаемое для всех маршрутов. Значение должно лежать в диапазоне от 1 до 255.

external *расстояние*

Административное расстояние OSPF, устанавливаемое для внешних маршрутов (маршрутов, полученных из другого протокола по перераспределению). Значение должно лежать в диапазоне от 1 до 255. Значение по умолчанию равно 110.

inter-area *расстояние*

Административное расстояние OSPF, устанавливаемое для межобластных маршрутов (маршрутов в другую область). Значение должно лежать в диапазоне от 1 до 255. Значение по умолчанию равно 110.

intra-area *расстояние*

Административное расстояние OSPF, устанавливаемое для внутриобластных маршрутов (маршрутов внутри области). Значение должно лежать в диапазоне от 1 до 255. Значение по умолчанию равно 110.

Значение по умолчанию

Административное расстояние по умолчанию для маршрутов OSPF равно 110.

Указания по использованию

Эта команда используется для установки административного расстояния, назначаемого маршрутам OSPF.

Административное расстояние отражает степень доверия к маршрутизатору или группе маршрутизаторов как к источнику маршрутной информации. В общем, чем больше значение, тем меньше степень доверия к элементу. Административное расстояние, равное 1, обычно означает непосредственно подключенную сеть, а равное 255 – неизвестный или ненадежный источник маршрутной информации. Обычно к OSPF применяется административное расстояние 110.

Форма **set** этой программы используется для установки административного расстояния.

Форма **delete** этой команды используется для восстановления значения административного расстояния по умолчанию.

Форма **show** этой команды используется для отображения настройки административного расстояния.

27.3.7 protocols ospf log-adjacency-changes

Включение или отключение протоколирования изменений в состоянии смежности для соседей.

Синтаксис

```
set protocols ospf log-adjacency-changes [detail]
delete protocols ospf log-adjacency-changes
show protocols ospf log-adjacency-changes
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   ospf {
      log-adjacency-changes {
         detail
      }
   }
}
```

Параметры

detail

Необязательный. Запись в журнал всех изменений состояния, не только изменений в состоянии смежности.

Значение по умолчанию

Запись в журнал изменений в состоянии смежности отключена. При использовании без ключевого слова detail в журнал записываются только изменения в состоянии смежности.

Указания по использованию

Эта команда используется для включения записи в журнал изменений в состоянии смежности.

Форма **set** этой команды используется для включения записи в журнал изменений в состоянии смежности.

Форма **delete** этой команды используется для отключения записи в журнал изменений в состоянии смежности.

Форма **show** этой команды используется для отображения настройки записи в журнал изменений в состоянии смежности.

27.3.8 protocols ospf max-metric router-lsa

Включение или отключение объявления максимального значения метрики на тупиковом маршрутизаторе OSPF при запуске или перезагрузке маршрутизатора.

Синтаксис

```
set protocols ospf max-metric router-lsa [administrative | on-shutdown <время> | on-startup <время>]

delete protocols ospf max-metric router-lsa [administrative | on-shutdown | on-startup]

show protocols ospf max-metric router-lsa [on-shutdown | on-startup]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    ospf {
        max-metric {
            router-lsa {
                administrative
                on-shutdown время
                on-startup время
            }
        }
    }
}
```

Параметры

administrative

Необязательный. Объявление максимальной метрики в течение неопределенного периода.

on-shutdown *время*

Объявление максимальной метрики при закрытии процесса OSPF. Указывает время в секундах, после которого объявление максимальной метрики должно быть прекращено и начато объявление обычной метрики OSPF, даже если

процесс стабилизации BGP еще не завершился. Значение должно лежать в диапазоне от 5 до 86400. Значение по умолчанию равно 600.

on-startup *время*

Объявление максимальной метрики при запуске или перезагрузке процесса OSPF. Указывает время в секундах, после которого объявление максимальной метрики должно быть прекращено и начато объявление обычной метрики OSPF, даже если процесс стабилизации BGP еще не завершился. Значение должно лежать в диапазоне от 5 до 86400. Значение по умолчанию равно 600.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для установки метрики, объявляемой маршрутизатором по LSA.

При помощи этой команды можно настроить маршрутизатор OSPF на объявление максимальной метрики другим маршрутизаторам, как описано в RFC 3137. Объявляя максимальную метрику, маршрутизатор фактически делает себя наименее предпочтительным в подсети для передачи другого трафика в другую подсеть. Во время периода наименьшей предпочтительности маршрутизатора таблицы BGP могут стабилизироваться, и маршрутизатор может быть корректно введен в эксплуатацию или выведен из нее без помех для трафика. Период объявления максимальной метрики заканчивается, если заканчивается стабилизация таблиц BGP либо если истекает время. С этого момента объявление максимальной метрики заменяется нормальной метрикой OSPF.

Форма **set** этой команды служит для включения объявления максимальной метрики.

Форма **delete** этой команды служит для отключения объявления максимальной метрики.

Форма **show** этой команды служит для отображения настройки объявления максимальной метрики.

27.3.9 protocols ospf mpls-te

Установка параметров управления направлением прохождения трафика при многопротокольной коммутации меток (MPLS-TE).

Синтаксис

```
set protocols ospf mpls-te [enable | router-address <ipv4-адрес>]
delete protocols ospf mpls-te [enable | router-address]
show protocols ospf mpls-te [router-address]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   ospf {
      mpls-te {
         enable
         router-address ipv4-адрес
      }
   }
}
```

Параметры

enable

Необязательный. Включение функциональности MPLS-TE.

ipv4-адрес

Необязательный. Стабильный IP-адрес объявляющего маршрутизатора.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для включения управления направлением прохождения трафика при многопротокольной коммутации меток (MPLS-TE).

Форма **set** этой команды используется для включения MPLS-TE.

Форма **delete** этой команды используется для удаления настройки MPLS-TE.

Форма **show** этой команды используется для отображения настройки MPLS-TE.

27.3.10 protocols ospf neighbor <ipv4-адрес>

Определение соседа по OSPF.

Синтаксис

```
set protocols ospf neighbor <ipv4-адрес> [poll-interval <интервал> | priority <приоритет>]

delete protocols ospf neighbor <ipv4-адрес> [poll-interval | priority]

show protocols ospf neighbor <ipv4-адрес> [poll-interval | priority]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   ospf {
      neighbor ipv4-адрес {
         poll-interval интервал
         priority приоритет
      }
   }
}
```

Параметры

ipv4-адрес

Обязательный. IPv4-адрес соседа по OSPF.

интервал

Необязательный. Интервал (в секундах) опроса соседа для подтверждения его достижимости. Значение должно лежать в диапазоне от 1 до 65535. Значение по умолчанию равно 120.

приоритет

Необязательный. Приоритет данного соседа. Значение должно лежать в диапазоне от 0 до 255, причем чем меньше значение, тем выше приоритет. Значение по умолчанию равно 1.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения соседа по OSPF и установки его характеристик.

Форма **set** этой команды используется для создания соседа по OSPF или изменения его характеристик.

Форма **delete** используется для удаления соседа по OSPF или сброса параметров соседа к значениям по умолчанию.

Форма **show** этой команды используется для настройки соседей по OSPF.

27.3.11 protocols ospf parameters

Установка глобальных параметров OSPF, таких как идентификатор маршрутизатора.

Синтаксис

```
set protocols ospf parameters [abr-type <тип> | opaque-lsa | rfc1583-compatibility | router-id <ipv4-адрес>]
```

```
delete protocols ospf parameters [abr-type | opaque-lsa | rfc1583-compatibility | router-id]
show protocols ospf parameters
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    ospf {
        parameters {
            abr-type тип
            opaque-lsa
            rfc1583-compatibility
            router-id ipv4-адрес      }
    }
}
```

Параметры

тип

Необязательный. Поддерживается только для граничных маршрутизаторов области (ABR). Установка типа ABR для OSPF. Поддерживаются следующие значения:

- cisco: выделение маршрутизатора как ABR Cisco;
- ibm: выделение маршрутизатора как ABR IBM;
- shortcut: выделение маршрутизатора как ABR, поддерживающего режим срезки;
- standard: выделение маршрутизатора как стандартного ABR.

Значение по умолчанию равно standard.

ПРИМЕЧАНИЕ В случае, когда Numa Edge является пограничным маршрутизатором и не имеет соединения с магистральной зоной, но имеет соединение с другим маршрутизатором, имеющим соединение с магистральной зоной, стандарт OSPF не позволяет Numa Edge использовать маршруты данного маршрутизатора. Данное ограничение применяется для предотвращения возникновения маршрутных петель.

При установке значения **cisco** или **ibm** параметра abr-type, Numa Edge получает возможность принимать сводки от других пограничных маршрутизаторов через немагистральные зоны, следовательно и осуществлять маршрутизацию данных через них, но только в случае отсутствия соединения с магистральной зоной.

Следует учитывать, что зоны, находящиеся между двумя маршрутизаторами в состоянии с полностью согласованной топологией (fully adjacent) считаются пригодными для транзита (transit capable), в связи с чем всегда могут быть использованы для маршрутизации трафика магистральной зоны в независимости как от состояния соединения между Numa Edge и магистральной зоны так и от значения параметра abr-type.

opaque-lsa

Необязательный. Включение поддержки объявления состояния непрозрачного канала в соответствии с описанием в RFC 2370.

rfc1583-compatibility

Необязательный. Включение соответствия спецификации RFC 1583 в отношении обработки внешних маршрутов AS.

ipv4-адрес

Необязательный. Явная установка идентификатора маршрутизатора с переопределением идентификатора маршрутизатора, вычисленного процессом OSPF. Используется формат IPv4-адреса.

Значение по умолчанию

По умолчанию поддержка непрозрачных LSA отключена. По умолчанию поддержка RFC 1583 отключена.

Если идентификатор маршрутизатора не настроен явно, процесс OSPF вычисляет идентификатор маршрутизатора по следующему алгоритму:

- используется IP-адрес интерфейса заглушки;
- используется наибольший из IP-адресов интерфейсов маршрутизатора;
- если никакие интерфейсы не определены, используется 0.0.0.0.

Указания по использованию

Эта команда используется для установки параметров, характерных для OSPF.

ПРИМЕЧАНИЕ После изменения идентификатора маршрутизатора происходит его перезагрузка.

Форма **set** этой команды используется для указания значений параметров.

Форма **delete** этой команды используется для восстановления значений по умолчанию глобальных параметров OSPF.

Форма **show** этой команды используется для отображения настройки глобальных параметров OSPF.

27.3.12 protocols ospf passive-interface <ethx>

Установка пассивного режима для указанного интерфейса.

Синтаксис

```
set protocols ospf passive-interface <ethx>
delete protocols ospf passive-interface <ethx>
show protocols ospf passive-interface
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   ospf {
      passive-interface ethx {
      }
   }
}
```

Параметры

ethx

Обязательный. Множественный узел. Интерфейс Ethernet, на котором следует установить пассивный режим.

Для того чтобы включить пассивный режим на нескольких интерфейсах, следует создать соответствующее количество узлов конфигурации passive-interface.

Значение по умолчанию

Пассивный режим не установлен.

Указания по использованию

Эта команда используется для установки пассивного режима на интерфейсе. При установке пассивного режима трафик OSPF может быть принят на интерфейсе, но не может быть отправлен через него.

Форма **set** этой команды используется для установки пассивного режима на интерфейсе.

Форма **delete** этой команды для отмены пассивного режима на интерфейсе.

Форма **show** этой команды используется для отображения настройки пассивного режима.

27.3.13 protocols ospf refresh timers <время>

Установка значений для таймеров обновления OSPF.

Синтаксис

```
set protocols ospf refresh timers <время>
delete protocols ospf refresh timers
show protocols ospf refresh timers
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   ospf {
      refresh {
         timers время
      }
   }
}
```

Параметры

время

Обязательный. Значение таймера в секундах. Значение должно лежать в диапазоне от 10 до 1800. Значение по умолчанию равно 1800 (30 минутам).

Значение по умолчанию

По умолчанию таймер обновления выставляется на 30 минут (1800 секунд).

Указания по использованию

Эта команда используется для установки значений таймера обновления состояния каналов OSPF.

Обновление состояния каналов - это механизм для проверки объявления состояния каналов (LSA) и сброса его давности до того, как она достигнет максимального значения. Когда период таймера обновления состояния каналов истекает, маршрутизатор рассылает новую информацию о состоянии каналов всем своим соседям, которые сбрасывают давность LSA.

Форма **set** этой команды используется для установки таймера обновления.

Форма **delete** этой команды используется для восстановления значения таймера обновления по умолчанию.

Форма **show** этой команды используется для отображения настройки таймера обновления.

27.3.14 protocols ospf timers throttle spf

Включение или отключение задержки вычислений SPF в OSPF.

Синтаксис

```
set protocols ospf timers throttle spf [delay <время> | initial-holdtime <время> | max-holdtime <время>]
delete protocols ospf timers throttle spf [delay | initial-holdtime | max-holdtime]
show protocols ospf timers throttle spf [delay | initial-holdtime | max-holdtime]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   ospf {
      timers {
         throttle {
            spf {
               delay время
               initial-holdtime время
               max-holdtime время
            }
         }
      }
   }
}
```

Параметры

delay *время*

Необязательный. Задержка (в мс) после получения первой информации об изменении топологии сети до расчета SPF. Значение должно лежать в диапазоне от 0 до 600000.

initial-holdtime *время*

Необязательный. Начальный интервал (в мс) между последовательными расчетами SPF. Значение должно лежать в диапазоне от 0 до 600000.

max-holdtime *время*

Необязательный. Максимальный интервал (в мс) между последовательными расчетами SPF. Значение должно лежать в диапазоне от 0 до 600000.

Значение по умолчанию

Задержка вычислений SPF отключена.

Указания по использованию

Эта команда используется для установки характеристик таймера для задержки вычислений SPF.

Расчеты предпочтительных кратчайших путей (SPF), в которых вычисляется дерево кратчайших путей (Shortest Path Tree, SPT), обычно выполняются при изменении топологи сети. Нестабильность сети может привести к избыточному количеству расчетов путей. Задержка вычисления SPF позволяет отложить вычисление SPF. Можно отложить первое вычисление и установить минимальный и максимальный интервал между вычислениями.

Форма **set** этой команды используется для включения задержки вычисления SPF и установки ее характеристик.

Форма **delete** этой команды используется для отключения задержки вычисления SPF.

Форма **show** этой команды используется для отображения настройки задержки вычисления SPF.

27.3.15 protocols ospf redistribute bgp

Установка параметров перераспределения маршрутов BGP на OSPF.

Синтаксис

```
set protocols ospf redistribute bgp [metric <метрика> | metric-type <тип> |
route-map <имя_карты>]

delete protocols ospf redistribute bgp [metric | metric-type | route-map]

show protocols ospf redistribute bgp [metric | metric-type | route-map]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   ospf {
      redistribute {
         bgp {
            metric метрика
            metric-type тип
            route-map имя_карты
         }
      }
   }
}
```

Параметры

метрика

Необязательный. Указанная метрика применяется к маршрутам BGP, перераспределяемым на OSPF. Значение должно лежать в диапазоне от 1 до 16. Значение по умолчанию равно 1.

тип

Необязательный. Способ вычисления стоимости. Поддерживаются значения 1 (внутренняя стоимость складывается с внешней стоимостью) и 2 (используется только внешняя стоимость). Значение по умолчанию равно 2.

имя_карты

Необязательный. Перераспределяются маршруты, удовлетворяющие указанной карте маршрутов.

Значение по умолчанию

Маршрутам BGP, перераспределяемым на OSPF, назначается значение метрики маршрутизации 1 и тип метрики 2. По умолчанию к перераспределяемым маршрутам BGP не применяется никакая карта маршрутов.

Указания по использованию

Эта команда используется для определения параметров перераспределения маршрутов BGP на OSPF.

Форма **set** этой команды используется для установки параметров перераспределения маршрутов BGP.

Форма **delete** этой команды используется для удаления параметров перераспределения маршрутов BGP.

Форма **show** этой команды используется для отображения настройки перераспределения маршрутов BGP.

27.3.16 protocols ospf redistribute connected

Установка параметров перераспределения непосредственно подключенных маршрутов на OSPF.

Синтаксис

```
set protocols ospf redistribute connected [metric <метрика> | metric-type <тип> | route-map <имя_карты>]

delete protocols ospf redistribute connected [metric | metric-type | route-map]

show protocols ospf redistribute connected [metric | metric-type | route-map]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   ospf {
      redistribute {
         connected {
            metric метрика
            metric-type тип
            route-map имя_карты
         }
      }
   }
}
```

Параметры

метрика

Необязательный. Указанная метрика применяется к непосредственно подключенным маршрутам, перераспределяемым на OSPF. Значение должно лежать в диапазоне от 1 до 16. Значение по умолчанию равно 1.

тип

Необязательный. Способ вычисления стоимости. Поддерживаются значения 1 (внутренняя стоимость складывается с внешней стоимостью) и 2 (используется только внешняя стоимость). Значение по умолчанию равно 2.

имя_карты

Необязательный. Перераспределяются маршруты, удовлетворяющие указанной карте маршрутов.

Значение по умолчанию

Непосредственно подключенным маршрутам, перераспределяемым на OSPF, назначается значение метрики маршрутизации 1 и тип метрики 2. По умолчанию к перераспределяемым непосредственно подключенным маршрутам никакие карты маршрутов не применяются.

Указания по использованию

Эта команда используется для определения параметров перераспределения непосредственно подключенных маршрутов на OSPF.

Форма **set** этой команды используется для установки параметров перераспределения непосредственно подключенных маршрутов.

Форма **delete** этой команды используется для удаления параметров перераспределения непосредственно подключенных маршрутов.

Форма **show** этой команды используется для отображения настройки перераспределения непосредственно подключенных маршрутов.

27.3.17 protocols ospf redistribute kernel

Установка параметров перераспределения маршрутов ядра на OSPF.

Синтаксис

```
set protocols ospf redistribute kernel [metric <метрика> | metric-type <тип>
| route-map <имя_карты>]

delete protocols ospf redistribute kernel [metric | metric-type | route-map]

show protocols ospf redistribute kernel [metric | metric-type | route-map]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   ospf {
      redistribute {
         kernel {
            metric метрика
            metric-type тип
            route-map имя_карты
         }
      }
   }
}
```

Параметры

метрика

Необязательный. Указанная метрика применяется к маршрутам ядра, перераспределяемым на OSPF. Значение должно лежать в диапазоне от 1 до 16. Значение по умолчанию равно 1.

тип

Необязательный. Способ вычисления стоимости. Поддерживаются значения 1 (внутренняя стоимость складывается со внешней стоимостью) и 2 (используется только внешняя стоимость). Значение по умолчанию равно 2.

имя_карты

Необязательный. Перераспределяются маршруты, удовлетворяющие указанной карте маршрутов.

Значение по умолчанию

Маршрутам ядра, перераспределяемым на OSPF, назначаются значение метрики маршрутизации 1 и тип метрики 2. По умолчанию к перераспределяемым маршрутам ядра никакие карты маршрутов не применяются.

Указания по использованию

Эта команда используется для определения параметров перераспределения маршрутов ядра на OSPF.

Форма **set** этой команды используется для установки параметров перераспределения маршрутов ядра.

Форма **delete** этой команды используется для удаления параметров перераспределения маршрутов ядра.

Форма **show** этой команды используется для отображения настройки перераспределения маршрутов ядра.

27.3.18 protocols ospf redistribute rip

Установка параметров перераспределения маршрутов RIP на OSPF.

Синтаксис

```
set protocols ospf redistribute rip [metric <метрика> | metric-type <тип> | route-map <имя_карты>]
delete protocols ospf redistribute rip [metric | metric-type | route-map]
show protocols ospf redistribute rip [metric | metric-type | route-map]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   ospf {
      redistribute {
```

```
            rip {
               metric метрика
               metric-type тип
               route-map имя_карты
            }
         }
      }
   }
```

Параметры

метрика

Необязательный. Указанная метрика применяется к маршрутам RIP, перераспределяемым на OSPF. Значение должно лежать в диапазоне от 1 до 16. Значение по умолчанию равно 1.

тип

Необязательный. Способ вычисления стоимости. Поддерживаются значения 1 (внутренняя стоимость складывается со внешней стоимостью) и 2 (используется только внешняя стоимость). Значение по умолчанию равно 2.

имя_карты

Необязательный. Перераспределяются маршруты, удовлетворяющие указанной карте маршрутов.

Значение по умолчанию

Маршрутам RIP, перераспределяемым на OSPF, назначаются значение метрики маршрутизации 1 и тип метрики 2. По умолчанию к перераспределяемым маршрутам RIP никакие карты маршрутов не применяются.

Указания по использованию

Эта команда используется для определения параметров перераспределения маршрутов RIP на OSPF.

Форма **set** этой команды используется для установки параметров перераспределения маршрутов RIP.

Форма **delete** этой команды используется для удаления параметров перераспределения маршрутов RIP.

Форма **show** этой команды используется для отображения настройки перераспределения маршрутов RIP.

27.3.19 protocols ospf redistribute static

Установка параметров перераспределения статических маршрутов на OSPF.

Синтаксис

```
set protocols ospf redistribute static [metric <метрика> | metric-type <тип>
| route-map <имя_карты>]
delete protocols ospf redistribute static [metric | metric-type | route-map]
show protocols ospf redistribute static [metric | metric-type | route-map]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   ospf {
      redistribute {
         static {
            metric метрика
            metric-type тип
            route-map имя_карты
```

```
            }
        }
    }
}
```

Параметры

метрика

Необязательный. Указанная метрика применяется к статическим маршрутам, перераспределяемым на OSPF. Значение должно лежать в диапазоне от 1 до 16. Значение по умолчанию равно 1.

тип

Необязательный. Способ вычисления стоимости. Поддерживаются значения 1 (внутренняя стоимость складывается со внешней стоимостью) и 2 (используется только внешняя стоимость). Значение по умолчанию равно 2.

имя_карты

Необязательный. Перераспределяются маршруты, удовлетворяющие указанной карте маршрутов.

Значение по умолчанию

Статическим маршрутам, перераспределяемым на OSPF, назначаются значение метрики маршрутизации 1 и тип метрики 2. По умолчанию к перераспределяемым статическим маршрутам никакие карты маршрутов не применяются.

Указания по использованию

Эта команда используется для определения параметров перераспределения статических маршрутов на OSPF.

Форма **set** этой команды используется для установки параметров перераспределения статических маршрутов.

Форма **delete** этой команды используется для удаления параметров перераспределения статических маршрутов.

Форма **show** этой команды используется для отображения настройки перераспределения статических маршрутов.

27.3.20 routing ospf debug enable event

Включение или отключение вывода отладочных сообщений, относящихся к событиям OSPF.

Синтаксис

```
routing ospf debug enable eventrouting ospf debug disable event
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для включения вывода сообщений уровня *trace*, относящихся к событиям OSPF.

Форма **disable** этой команды используется для отключения вывода отладочных сообщений для событий OSPF.

27.3.21 routing ospf debug enable ism

Включение или отключение вывода отладочных сообщений, относящихся к ISM в OSPF.

Синтаксис

```
routing ospf debug enable ism [events | status | timers]
routing ospf debug disable ism [events | status | timers]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

events

Необязательный. Включение или отключение вывода отладочных сообщений, относящихся к событиям ISM в OSPF.

status

Необязательный. Включение или отключение вывода отладочных сообщений, относящихся к статусу ISM в OSPF.

timers

Необязательный. Включение или отключение вывода отладочных сообщений, относящихся к таймерам ISM в OSPF.

Значение по умолчанию

При выдаче без параметра команда используется для включения или отключения всех сообщений ISM в OSPF.

Указания по использованию

Эта команда используется для включения вывода сообщений уровня *trace*, относящихся к событиям ISM в OSPF.

Форма **disable** этой команды используется для отключения вывода отладочных сообщений ISM в OSPF.

27.3.22 routing ospf debug enable lsa

Включение или отключение вывода отладочных сообщений, относящихся к объявлениям состояния канала (LSA) в OSPF.

Синтаксис

```
routing ospf debug enable lsa [flooding | generate | install | refresh]
routing ospf debug disable lsa [flooding | generate | install | refresh]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

flooding

Необязательный. Вывод сообщений, относящихся к событиям рассылки LSA в OSPF.

generate

Необязательный. Вывод сообщений, относящихся к созданию LSA в OSPF.

install

Необязательный. Вывод сообщений, относящихся к установке LSA в OSPF.

refresh

Необязательный. Вывод сообщений, относящихся к обновлениям LSA в OSPF.

Значение по умолчанию

При выдаче без параметра команда используется для включения отладочных сообщений о всех действиях по объявлению состояния каналов в OSPF.

Указания по использованию

Эта команда используется для включения вывода сообщений уровня *trace*, относящихся к объявлениям состояния каналов в OSPF.

Форма **disable** этой команды используется для отключения вывода отладочных сообщений, относящихся к объявлениям состояния каналов в OSPF.

27.3.23 routing ospf debug enable ospf nsm

Включение или отключение вывода отладочных сообщений, относящихся к NSM в OSPF.

Синтаксис

```
routing ospf debug enable nsm [events | status | timers]
routing ospf debug disable nsm [events | status | timers]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

events

Необязательный. Включение или отключение вывода отладочных сообщений, относящихся к событиям NSM в OSPF.

status

Необязательный. Включение или отключение вывода отладочных сообщений, относящихся к состоянию NSM в OSPF.

timers

Необязательный. Включение или отключение вывода отладочных сообщений, относящихся к таймерам NSM в OSPF.

Значение по умолчанию

При выдаче без параметра команда используется для включения или отключения всех сообщений NSM в OSPF.

Указания по использованию

Эта команда используется для включения вывода сообщений уровня *trace*, относящихся к событиям NSM в OSPF.

Форма **disable** этой команды используется для отключения вывода отладочных сообщений NSM в OSPF.

27.3.24 routing ospf debug enable nssa

Включение и отключение вывода отладочных сообщений, относящихся к малотупиковым областям (not-so-stubby areas, NSSA) в OSPF.

Синтаксис

```
routing ospf debug enable nssa
routing ospf debug disable nssa
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для включения вывода сообщений уровня *trace*, относящихся к малотупиковым областям (NSSA) в OSPF.

Форма **disable** этой команды используется для отключения вывода отладочных сообщений, относящихся к малотупиковым областям (NSSA) в OSPF.

27.3.25 routing ospf debug enable packet all

Включение или отключение вывода отладочных сообщений, относящихся ко всем типам пакетов OSPF.

Синтаксис

```
routing ospf debug enable all [all | recv [detail] | send [detail]]
routing ospf debug disable all [all | recv [detail] | send [detail]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

all

Необязательный. Вывод подробных отладочных сообщений для всех пакетов OSPF, как отправленных, так и полученных.

recv

Необязательный. Вывод отладочных сообщений для полученных пакетов OSPF всех типов.

send

Необязательный. Вывод отладочных сообщений для всех переданных пакетов OSPF.

detail

Необязательный. Вывод подробных отладочных сообщений.

Значение по умолчанию

Отладочные сообщения для всех типов пакетов OSPF выводятся со средним уровнем подробности.

Указания по использованию

Эта команда используется для включения вывода сообщений уровня *trace*, относящихся ко всем типам пакетов OSPF, приходящих на маршрутизатор и уходящих с него.

Форма **disable** этой команды используется для отключения вывода отладочных сообщений, относящихся ко всем типам пакетов OSPF.

27.3.26 routing ospf debug enable packet dd

Включение или отключение вывода отладочных сообщений, относящихся к пакетам описания базы данных (DD) протокола OSPF.

Синтаксис

```
routing ospf debug enable packet dd [all | recv [detail] | send [detail]]
routing ospf debug disable packet dd [all | recv [detail] | send [detail]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

all

Необязательный. Вывод подробных отладочных сообщений для всех пакетов DD протокола OSPF, как отправленных, так и полученных.

recv

Необязательный. Вывод отладочных сообщений для полученных пакетов DD протокола OSPF.

send

Необязательный. Вывод отладочных сообщений для переданных пакетов DD протокола OSPF.

detail

Необязательный. Вывод подробных отладочных сообщений.

Значение по умолчанию

Отладочные сообщения для пакетов DD протокола OSPF выводятся со средним уровнем подробности.

Указания по использованию

Эта команда используется для включения вывода сообщений уровня *trace*, относящихся к пакетам описания базы данных (DD) протокола OSPF. Пакеты DD протокола OSPF предоставляют сводку (резюме) каждого объявления состояния канала в базах данных состояний каналов. При синхронизации данных маршрутизаторы OSPF обмениваются такими пакетами.

Форма **disable** этой команды используется для отключения вывода отладочных сообщений, относящихся к пакетам DD протокола OSPF.

27.3.27 routing ospf debug enable packet hello

Включение или отключение вывода отладочных сообщений, относящихся к пакетам приветствия протокола OSPF.

Синтаксис

```
routing ospf debug enable packet hello [all | recv [detail] | send [detail]]
routing ospf debug disable packet hello [all| recv [detail] | send [detail]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

all

Необязательный. Вывод подробных отладочных сообщений для всех пакетов приветствия протокола OSPF, как отправленных, так и полученных.

recv

Необязательный. Вывод отладочных сообщений для полученных пакетов приветствия протокола OSPF.

send

Необязательный. Вывод отладочных сообщений для переданных пакетов приветствия протокола OSPF.

detail

Необязательный. Вывод подробных отладочных сообщений.

Значение по умолчанию

Отладочные сообщения для пакетов приветствия протокола OSPF выводятся со средним уровнем подробности.

Указания по использованию

Эта команда используется для включения вывода сообщений уровня *trace*, относящихся к пакетам приветствия протокола OSPF. Пакеты приветствия протокола OSPF отправляются с определенным интервалом для обнаружения соседей и подтверждения их достижимости. В пакетах приветствия содержатся сведения о конкретных таймерах OSPF, выделенном маршрутизаторе (DR), резервном выделенном маршрутизаторе (BDR) и известных соседях.

Форма **disable** этой команды используется для отключения вывода отладочных сообщений, относящихся к пакетам приветствия протокола OSPF.

27.3.28 routing ospf debug enable packet ls-ack

Включение или отключение вывода отладочных сообщений, относящихся к пакетам уведомления о состоянии канала (LS Ack) протокола OSPF.

Синтаксис

```
routing ospf debug enable packet ls-ack [all | recv [detail] | send [detail]]
```

```
routing ospf debug disable packet ls-ack [all | recv [detail] | send [detail]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

all

Необязательный. Вывод подробных отладочных сообщений для всех пакетов LS Ack протокола OSPF, как отправленных, так и полученных.

recv

Необязательный. Вывод отладочных сообщений для полученных пакетов LS Ack протокола OSPF.

send

Необязательный. Вывод отладочных сообщений для переданных пакетов LS Ack протокола OSPF.

detail

Необязательный. Вывод подробных отладочных сообщений.

Значение по умолчанию

Отладочные сообщения для пакетов LS Ack протокола OSPF выводятся со средним уровнем подробности.

Указания по использованию

Эта команда используется для включения вывода сообщений уровня *trace*, относящихся к пакетам LS Ack протокола OSPF. Пакеты LS Ack отправляются соседям по OSPF для подтверждения приема обновления к объявлению о состоянии каналов (пакета LSU) от соседа.

Форма **disable** этой команды используется для отключения вывода отладочных сообщений, относящихся к пакетам LS Ack протокола OSPF.

27.3.29 routing ospf debug enable packet ls-request

Включение или отключение вывода отладочных сообщений, относящихся к пакетам запроса состояния канала (LSR) протокола OSPF.

Синтаксис

```
routing ospf debug enable packet ls-request [all | recv [detail] | send [detail]]
```

```
routing ospf debug disable packet ls-request [all | recv [detail] | send [detail]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

all

Необязательный. Вывод подробных отладочных сообщений для всех пакетов LSR протокола OSPF, как отправленных, так и полученных.

recv

Необязательный. Вывод отладочных сообщений для полученных пакетов LSR протокола OSPF.

send

Необязательный. Вывод отладочных сообщений для переданных пакетов LSR протокола OSPF.

detail

Необязательный. Вывод подробных отладочных сообщений.

Значение по умолчанию

Отладочные сообщения для пакетов LSR протокола OSPF выводятся со средним уровнем подробности.

Указания по использованию

Эта команда используется для включения вывода сообщений уровня *trace*, относящихся к пакетам запроса состояния канала (LSR) протокола OSPF. После обмена пакетами DD соседние маршрутизаторы OSPF определяют, каких объявлений LSA недостает в локальной базе данных состояния каналов. Локальный маршрутизатор отправляет соседу пакет LSR с запросом на недостающие объявления LSA.

Форма **disable** этой команды используется для отключения вывода отладочных сообщений, относящихся к пакетам LSR протокола OSPF.

27.3.30 routing ospf debug enable packet ls-update

Включение или отключение вывода отладочных сообщений для пакетов обновления информации о состоянии канала (LSU) протокола OSPF.

Синтаксис

```
routing ospf debug ensable packet ls-update [all | recv [detail] | send [detail]]
```

```
routing ospf debug disable packet ls-update [all | recv [detail] | send [detail]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

all

Необязательный. Вывод подробных отладочных сообщений для всех пакетов LSU протокола OSPF, как отправленных, так и полученных.

recv

Необязательный. Вывод отладочных сообщений для полученных пакетов LSU протокола OSPF.

send

Необязательный. Вывод отладочных сообщений для переданных пакетов LSU протокола OSPF.

detail

Необязательный. Вывод подробных отладочных сообщений.

Значение по умолчанию

Отладочные сообщения для пакетов LSU протокола OSPF выводятся со средним уровнем подробности.

Указания по использованию

Эта команда используется для включения вывода сообщений уровня *trace*, относящихся к пакетам обновления информации о состоянии канала (LSR) протокола OSPF. В пакетах LSU соседу по OSPF передаются любые запрошенные обновления для LSA.

Форма **disable** этой команды используется для отключения вывода отладочных сообщений, относящихся к пакетам LSU протокола OSPF.

27.3.31 routing ospf debug enable zebra

Включение или отключение вывода отладочных сообщений для процесса Zebra, работающего с протоколом OSPF.

Синтаксис

```
routing ospf debug enable zebra [interface | redistribute]
```

```
routing ospf debug disable zebra [interface | redistribute]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

interface

Необязательный. Вывод отладочных сообщений для всех интерфейсов, на которых включен процесс Zebra, работающий с протоколом OSPF.

redistribute

Необязательный. Вывод отладочных сообщений для маршрутов, перераспределенных на протокол OSPF, с которым работает процесс Zebra.

Значение по умолчанию

Для действий, относящихся к процессу Zebra, работающему с протоколом OSPF, выводятся отладочные сообщения.

Указания по использованию

Эта команда используется для включения вывода сообщений уровня *trace*, относящихся к процессу Zebra, работающему с протоколом OSPF.

Форма **disable** этой команды используется для отключения вывода отладочных сообщений, относящихся к процессу Zebra, работающему с протоколом OSPF.

27.3.32 routing osfp debug status

Отображение флагов отладки протокола OSPF.

Синтаксис

```
routing ospf debug status
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствует.

Значение по умолчанию

Отсутствуют

Указания по использованию

Эта команда используется для вывода настроек режима отладки OSPF.

27.3.33 show ip ospf

Отображение высокоуровневых сведений о настройке OSPF.

Синтаксис

```
show ip ospf
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения высокоуровневых сведений об OSPF.

27.3.34 show ip ospf border-routers

Отображение сведений о граничных маршрутизаторах OSPF.

Синтаксис

```
show ip ospf border-routers
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения сведений о граничных маршрутизаторах OSPF.

27.3.35 show ip ospf database

Отображение сведений о базе данных OSPF.

Синтаксис

```
show ip ospf database [[asbr-summary | external | network | nssa-external | opaque-area | opaque-as | opaque-link | router | summary] [adv-router <ipv4-адрес>] | max-age | self-originate]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

asbr-summary

Отображение базы данных сводок граничных маршрутизаторов автономных систем (Autonomous System Border Router, ASBR) OSPF.

external

Отображение базы данных внешних маршрутов OSPF.

network

Отображение базы данных подсетей OSPF.

nssa-external

Отображение базы данных внешних NSSA OSPF.

opaque-area

Отображение базы данных непрозрачных областей OSPF.

opaque-as

Отображение базы данных непрозрачных автономных систем OSPF.

opaque-link

Отображение базы данных непрозрачных каналов OSPF.

router

Отображение базы данных маршрутизаторов OSPF.

summary

Отображение сводки базы данных OSPF.

ipv4-адрес

Необязательный. Отображение базы данных OSPF для данного адреса.

max-age

Отображение базы данных максимального возраста OSPF.

self-originate

Отображение базы данных маршрутов OSPF, созданных локальным маршрутизатором.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения сведений базы данных OSPF.

27.3.36 show ip ospf interface

Отображение сведений о настройке и состоянии OSPF для указанного интерфейса.

Синтаксис

```
show ip ospf interface [<интерфейс>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

интерфейс

Необязательный. Интерфейс, настройку и состояние которого требуется вывести.

Значение по умолчанию

Если интерфейс не указан, будут выведены сведения по всем интерфейсам.

Указания по использованию

Эта команда используется для отображения настройки OSPF на интерфейсе.

27.3.37 show ip ospf neighbor

Отображение сведений о соседях по OSPF для указанного адреса или интерфейса.

Синтаксис

```
show ip ospf neighbor [<интерфейс> | <ipv4-адрес> | detail | address <ipv4-адрес>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

интерфейс

Необязательный. Отображение сведений о соседях на указанном интерфейсе.

ipv4-адрес

Необязательный. Отображение сведений о соседе для указанного адреса.

detail

Необязательный. Отображение подробных сведений о соседях для всех соседей.

address *ipv4-адрес*

Необязательный. Отображение сведений о соседе для указанного адреса.

Значение по умолчанию

Если интерфейсы не указаны, будут выведены сведения по всем соседям.

Указания по использованию

Эта команда используется для отображения сведений о соседях по OSPF на указанном адресе или интерфейсе.

27.3.38 show ip ospf route

Отображение сведений о маршрутах OSPF.

Синтаксис

```
show ip ospf route
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения сведений о маршрутах OSPF.

27.3.39 show ip route ospf

Отображение всех маршрутов OSPF для IP.

Синтаксис

```
show ip route ospf
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения всех маршрутов OSPF на IP.

28 Настройка BGP

28.1 Настройка BGP

В этой главе рассматриваются следующие вопросы:

- обзор BGP;
- примеры настройки BGP;
- примеры настройки маршрутизации BGP с использованием IPv6.

28.1.1 Обзор BGP

В данном разделе представлены следующие темы:

- введение;
- iBGP и eBGP;
- процесс выбора BGP ID;
- процесс выбора пути BGP;
- масштабируемость BGP;
- колебания маршрута и демпфирование колебаний маршрута;
- путь AC;
- сообщества BGP;
- группы узлов;
- поддержка IPv4 и IPv6.

Введение

Протокол граничного шлюза (BGP) — основной протокол динамической маршрутизации, используемый в Интернете. С 1994 года действует четвёртая версия протокола, описанная в стандарте RFC 4271, все предыдущие версии являются устаревшими.

Основной функцией маршрутизаторов, поддерживающих протокол BGP, является обмен информацией о доступности подсетей между собой. Вместе с информацией о сетях передаются различные атрибуты этих сетей, с помощью которых BGP выбирает лучший маршрут и настраиваются политики маршрутизации.

Группа маршрутизаторов, которая работает под единым техническим и административным управлением и использует общую стратегию маршрутизации называется атономной системой (AC). Для обмена маршрутной информацией с другими AC, используется уникальный идентификатор, называемый номер AC (autonomous system number,ASN).

В первоначальном стандарте были описаны только 16-битные номера AC, то есть всего было доступно 65536 номеров. В стандарте RFC 4893 и затем в RFC 6793 были описаны методы применения 32-битных номеров AC.

Поскольку протокол BGP используется для глобальной связности в интернете, неккомерческая огранизация IANA («Администрация адресного пространства Интернет») контролирует назначение номеров AC. В таблице представлен перечень номеров AC и сценарии их использования, согласно рекомендациям IANA:

Таблица 213 – Перечень номеров AC

0	16	Зарезервировано для RPKI	RFC6483, RFC7607
1 - 23455	16	Публичные номера AC	
23456	16	Зарезервировано для трансляции 16-битных ASN в 32-битные	RFC6793
23457 - 64495	16	Публичные номера AC	
64496 - 64511	16	Используется для примеров и документации	RFC5398
64512 - 65534	16	Для приватного использования	RFC1930, RFC6996
65535	16	Зарезервировано/Не используется	RFC7300
65536 - 65551	32	Используется для примеров и документации	RFC4893, RFC5398
65552 - 131071	32	Зарезервировано/Не используется	
131072 - 4199999999	32	Публичные номера AC	

4200000000 - 4294967294	32	Для приватного использования	RFC6996
4294967295	32	Зарезервировано/Не используется	RFC7300

Публичные номера автономных систем распределяются между региональными интернет регистраторами (RIR), которые в свою очередь закрепляют номера АС за определенными огранизациями или пользователями. Для России и Европпы региональным регистратором является RIPE NCC.

BGP является протоколом прикладного уровня и функционирует поверх протокола транспортного уровня TCP (порт номер 179). После установки соединения передаётся информация обо всех маршрутах, предназначенных для экспорта. В дальнейшем передаётся только информация об изменениях в таблицах маршрутизации. При закрытии соединения удаляются все маршруты, информация о которых передана противоположной стороной.

Маршрутная информация, передаваемая с использованием BGP, поддерживает только парадигму пересылки на основе адреса получателя, которая предполагает, что пересылка пакетов происходит на основании адреса получателя, содержащегося в заголовке IP-пакета. Это, в свою очередь, отражает набор правил политики, которые могут применяться (или не применяться) с использованием BGP.

Маршрутизаторы, настроенные на соединение через протокол BGP, называются узлами BGP или соседями BGP.

Маршрутизаторы, относящиеся к одной и той же АС, называются внутренними узлами BGP (internal BGP – iBGP).

Маршрутизаторы, относящиеся к разным АС, называются внешними узлами BGP (external BGP – eBGP).

Есть два основных типа обмена маршрутами BGP между узлами: анонсирование одного нового маршрута и отзыв группы маршрутов. При этом, анонсирование и отзыв могут происходить одновременно.

- посредством анонсирования маршрута узлу передаётся информация о возможности достижения определённой подсети посредством данного маршрута, а также информация об атрибутах данного пути;
- посредством отзыва маршрута узлу передаётся информация о невозможности достижения ранее анонсированного маршрута.

Все действующие анонсированные маршруты, полученные маршрутизатором, использующим BGP, помещаются в таблицу маршрутизации BGP. Эти маршруты называются путями BGP. Таким образом, для каждого конкретного префикса подсети в таблице маршрутизации BGP может содержаться несколько разных маршрутов — по одному на каждый узел BGP. Для определения оптимального маршрута используется процесс выбора маршрута. Процесс выбора маршрута запускается после обновления информации и служит как для отбора маршрутов, предназначенных для локального использования, так и для маршрутов, подлежащих передаче другим маршрутизаторам. Процесс использует атрибуты полученных маршрутов для установки предпочтительности маршрута, либо для исключения маршрута из процесса отбора. Процесс делится на три фазы:

- вычисление предпочтительности каждого полученного маршрута;
- выбор наилучшего маршрута для каждого места назначения и занесение его в активную таблицу маршрутизации;
- передача маршрутов на другие маршрутизаторы, при этом может производиться суммирование маршрутов.

Одним из основных атрибутов пути BGP является AS_PATH. Данный атрибут служит для идентификации АС и построения графа связности автономных систем, через которые передаются данные. Граф связности АС используется для предотвращения появления маршрутных петель. Атрибут AS_PATH читается справа налево, первое число (крайнее правое) обозначает номер АС, в которой находится данный префикс подсети. Данная автономная система является первой АС, анонсировавшей маршрут и называется АС происхождения. Например, в значении атрибута

```
AS_PATH 4 3 2 1
```

АС 1 — это АС происхождения, которая отправила анонс для АС 2, АС 2 отправила анонс для АС 3, которая в свою очередь отправила анонс для АС 4. Также, атрибутами пути BGP являются ORIGIN, NEXT_HOP, MULTI_EXIT_DISC (multi-exit discriminator), LOCAL_PREF (local preference), ATOMIC_AGGREGATE и AGGREGATOR. Более подробное описание данных атрибутов находится далее по тексту.

iBGP и eBGP

Все узлы узлы BGP можно отнести к двум группам:

- внутренние узлы BGP (iBGP – internal BGP. Узлы, относящиеся к одной и той же АС);
- внешние узлы BGP (eBGP – external BGP. Узлы, относящиеся к разным АС).

iBGP

Согласно спецификации RFC 4271, все узлы iBGP должны быть соединены друг с другом в рамках одной АС («каждый с каждым»), таким образом создавая полную ячеистую топологию соединений iBGP и обеспечивая пиринг (исключением являются АС, настроенные по методу отражения маршрутов. В таком случае, если один из узлов iBGP анонсирует префикс подсети для других узлов iBGP, то путь АС не изменяется (атрибут AS_PATH остаётся тем же). Реализация полной ячеистой топологии требует, чтобы все узлы BGP содержали одинаковые таблицы BGP, кроме случаев применения разных политик маршрутизации для некоторых узлов.

Когда маршрутизатор получает анонс узла iBGP, процесс BGP использует алгоритм выбора наилучшего маршрута для того, чтобы определить является ли данный путь оптимальным для заданного префикса. Если данный путь является оптимальным, то процесс BGP использует его в качестве кандидата на включение в таблицу маршрутизации, после чего путь анонсируется для всех остальных узлов BGP (как для iBGP, так и для eBGP). Если данный путь не является оптимальным, то процесс BGP сохраняет его копию в таблице BGP для использования при дальнейших вычислениях оптимального пути в случае изменения информации о доступных маршрутах для заданного префикса (например в случае отзыва текущего «оптимального пути»).

BGP ID – это уникальный идентификатор, имеющий формат IP-адреса, используемый для идентификации узлов BGP. При этом помимо BGP ID, каждый узел BGP имеет IP-адрес, используемый для непосредственного соединения с другими узлами BGP.

Для осуществления пиринга между узлами iBGP, IP-адрес и BGP ID привязываются к интерфейсу заглушки (loopback). Сессия iBGP проходит в рамках локальной сети с избыточными физическими соединениями между устройствами iBGP. Интерфейс заглушки является достижимым в случае функционирования хотя бы одного физического интерфейса, что, в совокупности с избыточностью физических или логических соединений между узлами iBGP, делает его оптимальным при выборе интерфейса для обеспечения пиринга между узлами iBGP.

Так как протокол BGP не предусматривает обмена информации о достижимости отдельных узлов BGP в рамках одной АС, каждый узел iBGP должен использовать внутренний протокол шлюза (Interior Gateway Protocol – IGP). В качестве маршрута IGP может выступать маршрут на базе физического соединения (connected route), статический маршрут, либо маршрут через динамический протокол маршрутизации (например, RIP или OSPF).

eBGP

Согласно спецификации RFC 4271, соединение между двумя узлами eBGP, принадлежащими к разным АС, обеспечивает связь между этими АС. Обычно, узлы eBGP соединяются через порт WAN, таким образом, между двумя узлами eBGP существует только одно физическое соединение. Однако, в целях обеспечения избыточности соединения или для реализации механизмов балансировки нагрузки возможно использование нескольких соединений между двумя узлами eBGP.

При построении графа связности автономных систем для определённого префикса используется атрибут AS_PATH. Когда префикс анонсируется узлу eBGP, то к атрибуту AS_PATH добавляется номер локальной АС, к которой относится данный узел. Если узел eBGP получает анонс префикса, содержащий номер локальной АС (АС к которой принадлежит данный узел), то данный узел отвергает этот анонс. Анонсы префиксов, полученные от узлов eBGP, также используются в процессе выбора оптимального пути BGP.

Обычно для узлов eBGP, в качестве IP-адрес и BGP ID выступает IP-адрес интерфейса маршрутизатора, используемого для физического соединения устройств eBGP. Однако если используется несколько интерфейсов для обеспечения соединения eBGP между двумя устройствами, то в качестве BGP ID используется IP-адрес интерфейса заглушки, а в качестве IP-адреса для непосредственного соединения в рамках eBGP используется адрес физического интерфейса.

Процесс выбора BGP ID

BGP ID – это четырёхоктетное целое число без знака, являющееся BGP идентификатором отправителя указанного сообщения. Узел BGP устанавливает в качестве идентификатора BGP IP-адрес, присвоенный данному узлу BGP. Значение идентификатора BGP определяется при старте узла и совпадает для всех локальных интерфейсов и самого узла BGP.

В Numa Edge, возможно как автоматическое создание BGP ID, так и непосредственное указание посредством использования команды protocols bgp <номер_ас> parameters router-id <идентификатор>. Если выбрано автоматическое определение BGP ID, то в качестве значения используется IP-адрес с интерфейса заглушки, при условии, что этот адрес не 127.0.0.1. Если адрес на интерфейсе заглушки отсутствует, то в качестве BGP ID используется первый IP-адрес с настроенного на устройстве интерфейса.

Оптимальным способом указания BGP ID является присвоение IP-адреса с маской /32 интерфейсу заглушки с последующим указанием данного адреса в качестве BGP ID.

Процесс выбора пути BGP

Процесс BGP может получать анонс одного и того же префикса от нескольких узлов одновременно. Каждый такой анонс называется путем. Процесс BGP выбирает «лучший» путь из доступных, после чего этот путь становится кандидатом в маршруты протокола BGP (то есть кандидатом на включение его в информационную базу маршрутизации (Routing Information Base – RIB)).

Факт наличия или отсутствия у других протоколов кандидатов в маршруты для данного префикса сети влияет на включение маршрута информационную базу маршрутизации. Приоритет включения маршрута в информационную базу маршрутизации определяется административной стоимостью процесса, выдвигающего данный маршрут в качестве кандидата: чем она меньше, тем большим приоритетом обладает процесс. Например, если в качестве кандидата для одного и того же префикса одновременно выступают статический маршрут и маршрут BGP, то в информационную базу будет включен только статический маршрут, так как процесс статической маршрутизации имеет меньшую административную стоимость, чем процесс BGP.

Следует отметить, что процесс BGP не учитывает пути, у которых адрес, указанный в качестве значения атрибута NEXT_HOP недостижим посредством маршрутов, указанных в RIB. Согласно спецификации RFC 4271, выбор пути BGP происходит с учётом следующих критериев:

- **LOCAL_PREF**: более предпочтительным считается путь с наибольшим значением данного атрибута;
- **AS_PATH**: более предпочтительным считается самый короткий путь (путь с меньшим количеством символов в значении данного атрибута);
- **ORIGIN**: более предпочтительным считается путь с более низким типом ORIGIN;
- **MULTI_EXIT_DISC**: более предпочтительным считается путь с меньшим значением данного атрибута;
- **Тип узла**: более предпочтительным считается путь через узлы eBGP;
- **Метрика IGP**: более предпочтительным считается путь с меньшей метрикой IGP для адреса, указанного в качестве значения атрибута NEXT_HOP;
- **BGP_ID**: более предпочтительным считается путь с меньшим значением данного атрибута;
- **IP-адрес узла**: более предпочтительным считается путь с меньшим значением IP-адреса.

Сравнение путей осуществляется по каждому критерию по порядку, указанному выше, до тех пор, пока не будет установлено первое отличие. Например, если два пути имеют одинаковое значение атрибуте LOCAL_PREF, но разные значения атрибута AS_PATH, то «лучшим» будет выбран путь с меньшим количеством символов в значении данного атрибута. Таким образом, если происходит сравнение IP-адресов узлов, это значит, что по всем остальным критериям сравниваемые узлы равнозначны.

Для просмотра списка выбранных путей используется команда show ip bgp.

Масштабируемость BGP

Согласно спецификации RFC 4271, все узлы iBGP должны быть соединены друг с другом в рамках одной АС («каждый с каждым»), таким образом, создавая полную ячеистую топологию соединений iBGP. Результатом этого является необходимость поддержки каждым узлом BGPn·(n-1)2уникальных сессий iBGP, где n – число узлов автономной системы. Подобную АС невозможно эффективно масштабировать, так как при наличии нескольких сотен маршрутизаторов подобная структура характеризуется сложностью настройки каждого элемента и избыточностью физических соединений.

Для решения проблемы масштабируемости протокол BGP поддерживает следующие расширения:

- конфедерация автономных систем в BGP (RFC 3065);
- отражение маршрутов BGP (RFC 2796).

Конфедерация автономных систем в BGP

В конфедерации автономных систем BGP, одна автономная система разбивается не несколько автономных подсистем. Каждой автономной подсистеме присваивается собственный номер (AS Confederation ID). Для этих целей можно взять любой номер из приватного диапазона допустимых значений АС от 64512 до 65534. Каждый узел автономной подсистемы использует номер автономной подсистемы в качестве номера АС при установке соединения с внешними узлами, то есть номер автономной подсистемы является номером АС для узлов, не состоящих в данной конфедерации. Этот номер анонсируется в качестве значения атрибута AS_PATH при построении графа связности автономных систем.

Также каждому узлу автономной подсистемы присваивается номер члена АС (Member AS Number), который используется при установке соединения с узлами, входящими в данную автономную подсистему.

Внутри автономной подсистемы используются соединения iBGP. Для соединения между двумя автономными подсистемами используются соединения eBGP. При этом для внешних узлов, автономные подсистемы, сгруппированные в конфедерацию, являются единой АС.

На рисунке показана АС, состоящая из девяти узлов iBGP, соединённых по схеме «каждый с каждым».

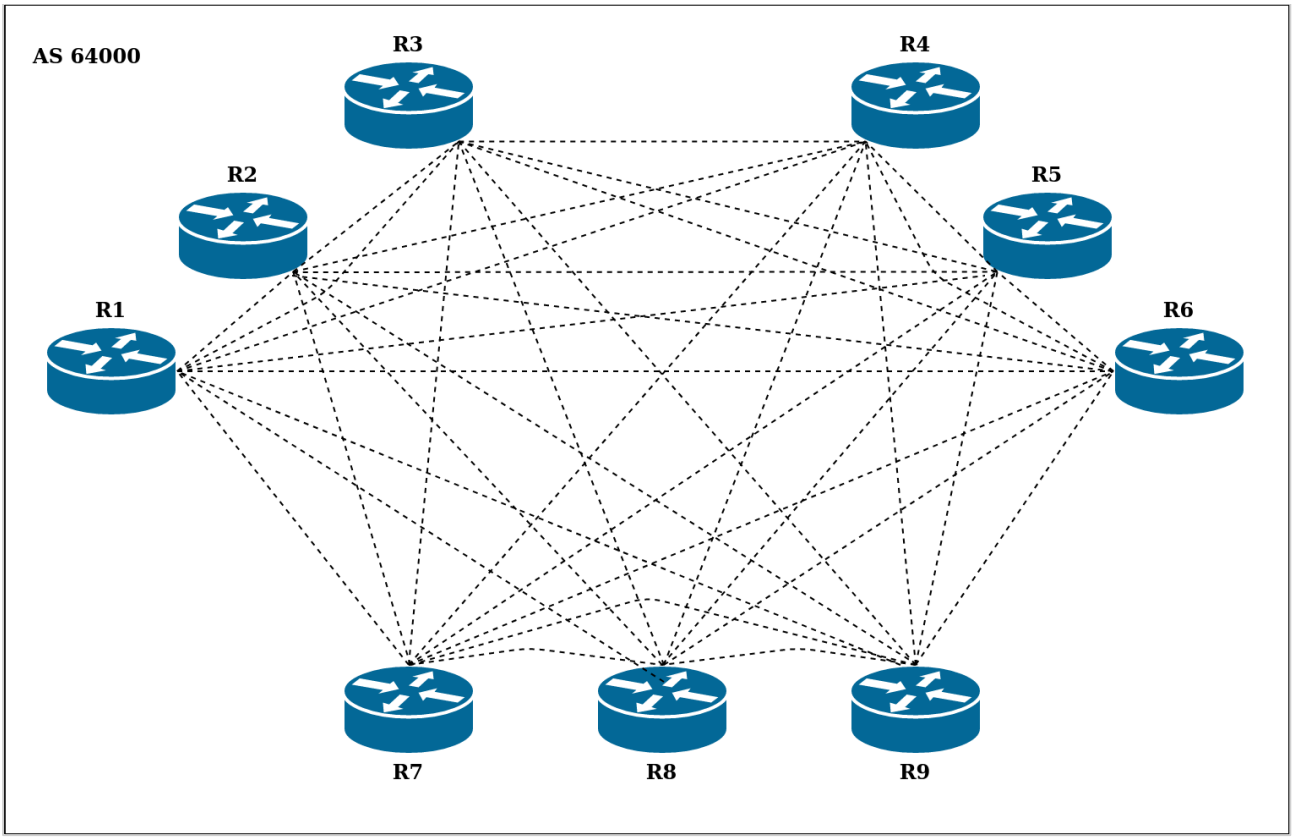


Рисунок 61 – Схема соединения iBGP «каждый с каждым».

На рисунке показано разделение АС на три автоматизированные подсистемы, образующие конфедерацию. Внутри автоматизированной подсистемы узлы соединены по схеме «каждый с каждым», сами же подсистемы соединены посредством eBGP.

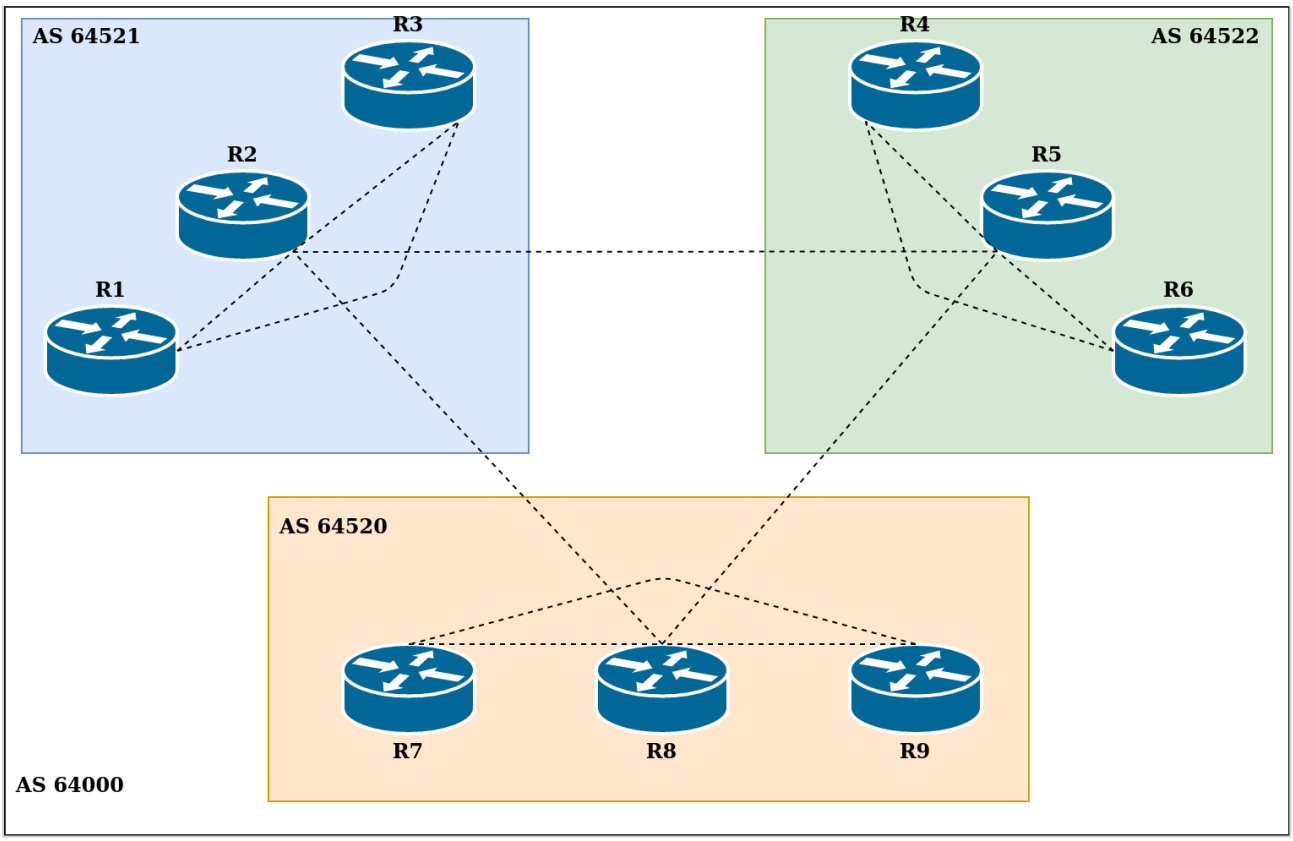


Рисунок 62 – Конфедерация BGP

Отражение маршрутов BGP

Данное расширение позволяет нескольким узлам iBGP взаимодействовать с центральным узлом, действующим в качестве маршрутного отражателя (route reflector server), при этом остальные узлы iBGP выступают в роли клиентов отражателя маршрутов (route reflector clients). Таким образом, один из узлов BGP получает возможность анонсировать полученные маршруты другим узлам iBGP. Каждый узел iBGP может соединяться с одним или несколькими отражателями маршрутов.

С точки зрения маршрутного отражателя, внешние узлы подразделяются на клиенты (client peers) и неклиенты (non-client peers). Маршрутный отражатель вместе со своими клиентами формирует кластер. Все узлы, не вошедшие в кластер, являются неклиентами для данного отражателя маршрутов.

Неклиенты должны соединяться друг с другом и с отражателем маршрутов, так как они работают в соответствии со стандартными правилами анонсирования маршрутов BGP, при этом отсутствует необходимость наличия соединения с узлами, являющимися клиентами отражателя маршрутов. Клиенты не должны взаимодействовать с неклиентами вне кластера, к которому они принадлежат.

Внутри кластера, каждый клиент должен соединяться посредством iBGP с одним или несколькими отражателями маршрутов. При этом отсутствует необходимость наличия соединения между клиентами внутри кластера.

Функция отражения маршрутов реализована только в самом маршрутном отражателе. Таким образом, клиенты и неклиенты отражателя маршрутов представляют собой обычные узлы BGP, в которых отсутствуют какие-либо настройки отражателя маршрутов. Узлы BGP считаются клиентами определённого отражателя маршрутов при условии присутствия в списке клиентов данного отражателя маршрутов.

Отражатель маршрутов, получающий несколько маршрутов для одного и того же префикса, использует стандартный процесс выбора пути BGP. После выбора «наилучшего» пути, этот путь будет распространяться внутри AC на основании следующих правил:

- если маршрут получен от неклиента, то он будет отражен только клиентам;
- если маршрут получен от клиента, то он будет отражен всем узла, как клиентам, так и неклиентам;
- если маршрут получен от узла eBGP, то он будет отражен всем узлам, как клиентам, так и неклиентам.

На рисунке показана схема подключения узлов BGP с применением отражения маршрутов.

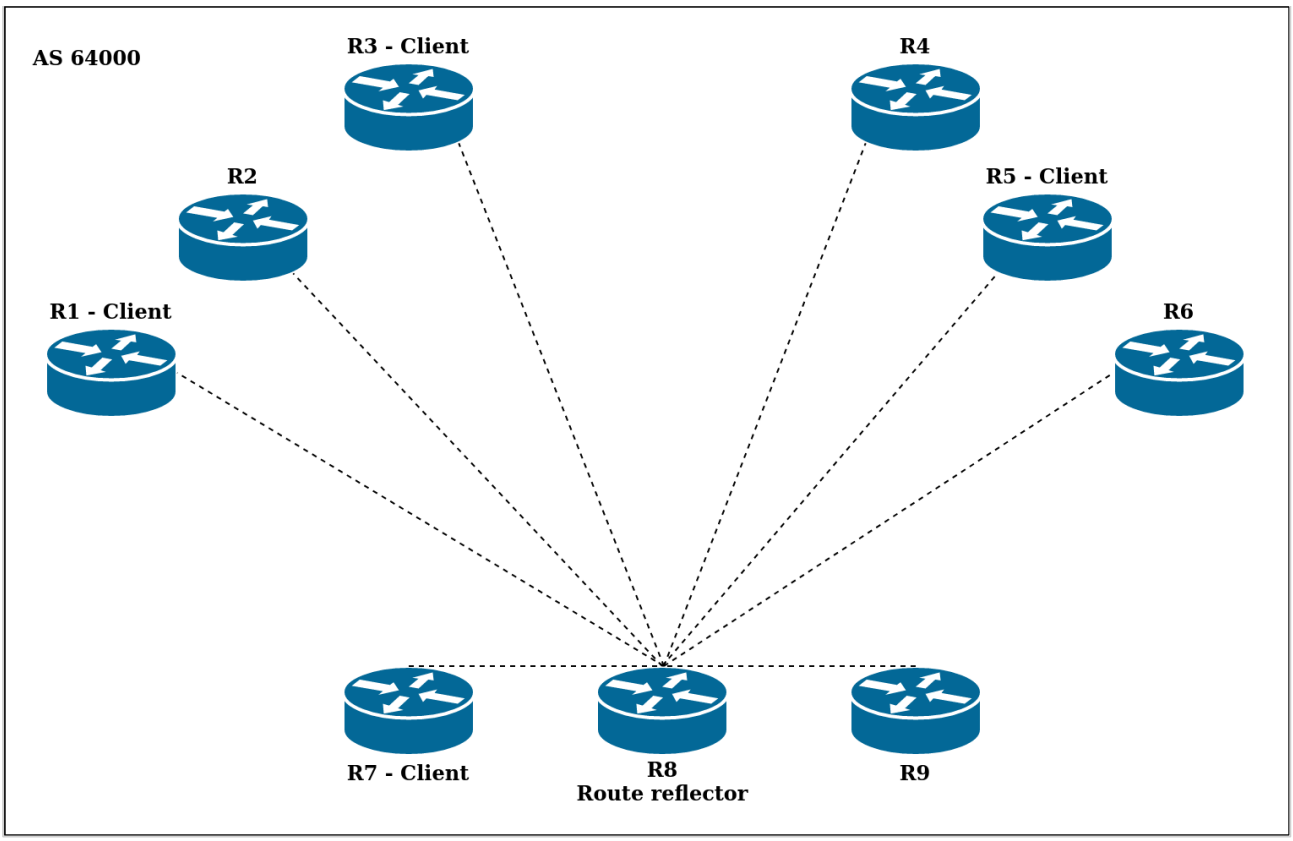


Рисунок 63 – Отражение маршрутов iBGP

При использовании отражения маршрутов BGP, крайне важно обеспечение избыточности и надежности, так как при выходе из строя отражателя маршрутов, клиенты, состоящие в кластере, оказываются изолированными от остальной сети. Для удовлетворения требований избыточности, рекомендуется организовывать несколько отражателей маршрутов в рамках одного кластера. Таким образом, клиенты смогут одновременно взаимодействовать с несколькими отражателями маршрутов. Если один из отражателей выходит из строя, то другой будет выполнять его функции. При этом в первую очередь следует обеспечивать физическую избыточность, так как логическая избыточность не имеет практической пользы при использовании метода отражения маршрутов.

Следует отметить, что для предотвращения возникновения петель маршрутизации, клиенты отражателя маршрутов не должны иметь соединения с отражателем маршрутов вне кластера.

Колебания маршрута и демпфирование колебаний маршрута

Одной из характеристик производительности сети BGP является колебание маршрута. В больших сетях довольно распространенным для таблиц маршрутизации BGP является частое обновление, поскольку подключения то возникают, то пропадают. Однако для любого конкретного маршрутизатора такой тип активности может быть относительно частым. При некорректной настройке маршрутизатора, подобное поведение ведет к повторяющимся и избыточным циклам отключения и подключения. При первичном или повторном подключении маршрутизатора к АС, для всех участников данной АС запускается процесс выбора наилучшего маршрута, информация о появлении нового маршрута рассылается всем узлам АС. Данные действия совершаются при каждом включении/отключении маршрутизатора, что конечном итоге приводит к большой кратковременной загрузке ЦП всех маршрутизаторов, состоящих в данной АС. Это явление называется колебанием маршрута. Для решения данной проблемы архитектура BGP предусматривает возможность применения демпфирования колебания маршрута.

Демпфирование колебания маршрута (Route flap damping) представляет собой механизм ограничения распространения сообщений об обновлении маршрутной информации между узлами BGP для колеблющихся маршрутов, не затрагивая обновление маршрутной информации для стабильных маршрутов.

При включении демпфирования колебаний маршрутов, каждому маршруту в сети BGP назначается параметр **suppress**. При каждом колебании (каждый раз, когда маршрут анонсируется и отзывается в течение короткого промежутка времени) увеличивается значение данного параметра. Если значение параметра **suppress** превысит 1000, то данный маршрут подавляется (узлам BGP запрещается использование данного маршрута). При этом, если маршрут остаётся стабильным в течении промежутка времени, заданного в качестве

значения параметра **half-life**, то значение параметра **suppress** уменьшается в два раза. После того, как значение параметра **suppress** достигнет минимального порогового значения, заданного параметром **re-use**, то данный маршрут перестаёт считаться подавленным (узлам BGP вновь разрешается использовать данный маршрут.)

Значение, на которое может увеличиться параметр **suppress** за одно колебание маршрута, автоматически рассчитывается по формуле:

```
reuse * 2max-supress-timehalf-life.
```

Если маршрут «подавлен», все анонсы и отзывы данного маршрута игнорируются узлами BGP. Это помогает локализовать колебание маршрута в рамках определённого соединения между узлами.

Путь AC

Путём AC называют маршрут между автономными системами BGP, который необходимо пройти пакету для достижения заданного узла назначения. Путь AC представляет собой последовательность номеров AC. Номер AC — это уникальный идентификатор автономной системы. Каждый номер AC представляет автономную систему, через которую проходит пакет при использовании определённого маршрута для достижения узла назначения. Путь AC указан в атрибуте AS_PATH. Для достижения узла назначения по заданному пути AC, пакет должен пройти все AC с номерами, указанными в атрибуте AS_PATH, от последнего (крайнего левого) к первому (крайнему правому). Крайний правый номер AC, указанный в атрибуте AS_PATH, и является AC назначения.

Для полного или частичного изменения пути AC в Numa edge используются политики маршрутизации BGP, реализуемые посредством использования регулярных выражений в параметре **as-path** или создания именного набора регулярных выражений пути AC, а также посредством использования параметра **as-path-list** и указания имени при выполнении команды.

По умолчанию Numa edge использует атрибут AS_PATH при выборе наилучшего пути в стандартной конфигурации и не использует при применении конфедерации. Правила использования или не использования атрибута AS_PATH при выборе наилучшего пути, в том или ином случае, можно задать посредством команды protocols bgp <номер_ac> parameters bestpath as-path.

Сообщества BGP

Протокол BGP поддерживает правила транзита с помощью контролируемого распределения маршрутной информации. Однако контроль за распространением маршрутной информации основан только на адресных префиксах IP, или на значении атрибута AS_PATH (или его части).

Для облегчения и упрощения контроля за маршрутной информацией используется группировка адресатов, образующих сообщества BGP. Таким образом маршрутизация может осуществляться с учётом этих сообществ. Подобная схема существенно упрощает конфигурацию узлов BGP в части контроля за распространением маршрутной информации.

Сообществом (группой) BGP называют группу адресатов с неким общим свойством. Общее свойство определяется администратором автономной системы (администратор может определить, к какому сообществу относится тот или иной адресат). По умолчанию все адресаты относятся к сообществу «INTERNET».

Все обновления BGP имеют атрибут COMMUNITIES, называемый атрибутом пути сообществ. Он относится к числу необязательных переходных атрибутов переменной длины. COMMUNITIES представляет из себя набор четырехоктетных значений, каждое из которых определяет сообщество. Все маршруты с таким атрибутом относятся к сообществам, указанным в атрибуте.

Идентификатором сообщества является 32-битное число, в котором первые два октета являются номером автономной системы, а остальные — произвольным значением, определяющимся автономной системой. Значения в диапазоне от 0x0000000 до 0x0000FFFF и от 0xFFFF0000 до 0xFFFFFFFF являются зарезервированными. Остальные значения нужно кодировать с использованием номера автономной системы в качестве двух первых октетов.

Существует два типа сообществ BGP: общепринятые сообщества и частные сообщества. Спецификация RFC 1997 определяет следующие типы общепринятых сообществ:

- **NO_EXPORT (0xFFFFFF01)** : Все маршруты, содержащие данное значение в атрибуте COMMUNITY, не анонсируются за пределы конфедерации BGP (отдельные автономные системы, не входящие в конфедерацию, в этом случае рассматриваются как конфедерации).

- **NO_ADVERTISE (0xFFFFFF02)** : Все маршруты, содержащие данное значение в атрибуте COMMUNITY, не анонсируются другим узлам BGP.

- **LOCAL_AS (0xFFFFFF03)**: Все маршруты, содержащие данное значение в атрибуте COMMUNITY, анонсируются только узлам iBGP.
- **INTERNET**: Все маршруты, содержащие данное значение в атрибуте COMMUNITY, анонсируются всем узлам без ограничений (данное сообщество не описано в спецификации RFC 1997).

Следует учитывать, что узел BGP, получивший маршрут без атрибута COMMUNITIES, может добавить такой атрибут при дальнейшем распространении маршрута другим узлам BGP. При этом, узел BGP, получивший маршрут с атрибутом COMMUNITIES, может изменить этот атрибут в соответствии с локальной политикой.

Группы узлов

При возникновении необходимости настройки нескольких узлов BGP с одинаковыми параметрами, в Numa Edge возможно использование групп узлов. Настройка групп узлов происходит таким же образом, как настройка отдельных узлов. При применении какой-либо настройки к группе узлов, данная настройка применяется ко всем узлам, состоящим в данной группе. Создание группы узлов осуществляется посредством команды `protocols bgp <asn> peer-group <group-name>`.

Добавление определённого узла в группу узлов осуществляется с помощью команды `protocols bgp <asn> neighbor <id> peer-group <group-name>`.

Поддержка IPv4 и IPv6

В Numa Edge доступна настройка следующих возможностей:

- сессия BGP между узлами BGP по протоколу IPv4;
- сессия BGP между узлами BGP по протоколу IPv6;
- доставка маршрутной информации по протоколу IPv4 может осуществляться как через узлы, использующие протокол IPv4, так и через узлы, использующие протокол IPv6;
- доставка маршрутной информации по протоколу IPv6 может осуществляться как через узлы, использующие протокол IPv4, так и через узлы, использующие протокол IPv6;
- доставка маршрутной информации как по протоколу IPv4, так и по протоколу IPv6, может осуществляться в рамках одной сессии BGP между узлами BGP по протоколу IPv4 или IPv6.

ПРИМЕЧАНИЕ Маршруты IPv4 в рамках IPv6-сессии, как и маршруты IPv6 в рамках IPv4-сессии не отображаются посредством команды **show**.

Обмен маршрутами IPv4 может осуществляться после включения BGP в Numa Edge посредством использования команды `protocols bgp <номер_ас>`.

Обмен маршрутами IPv6 может осуществляться после включения использования однонаправленных маршрутов BGP поверх IPv6 (посредством применения команды `protocols bgp <номер_ас> address-family ipv6-unicast`), добавления соседнего узла BGP с однонаправленным IPv6-адресом (посредством применения команды `protocols bgp <asn> neighbor <id> address-family ipv6-unicast`), либо добавления группы узлов BGP, поддерживающих однонаправленную передачу поверх протокола IPv6 (посредством применения команды `protocols bgp <asn> peer-group <group-name> address-family ipv6-unicast`).

28.1.2 Примеры настройки BGP

В данной главе рассматриваются различные примеры настройки сети BGP, схема которой показана на рисунке.

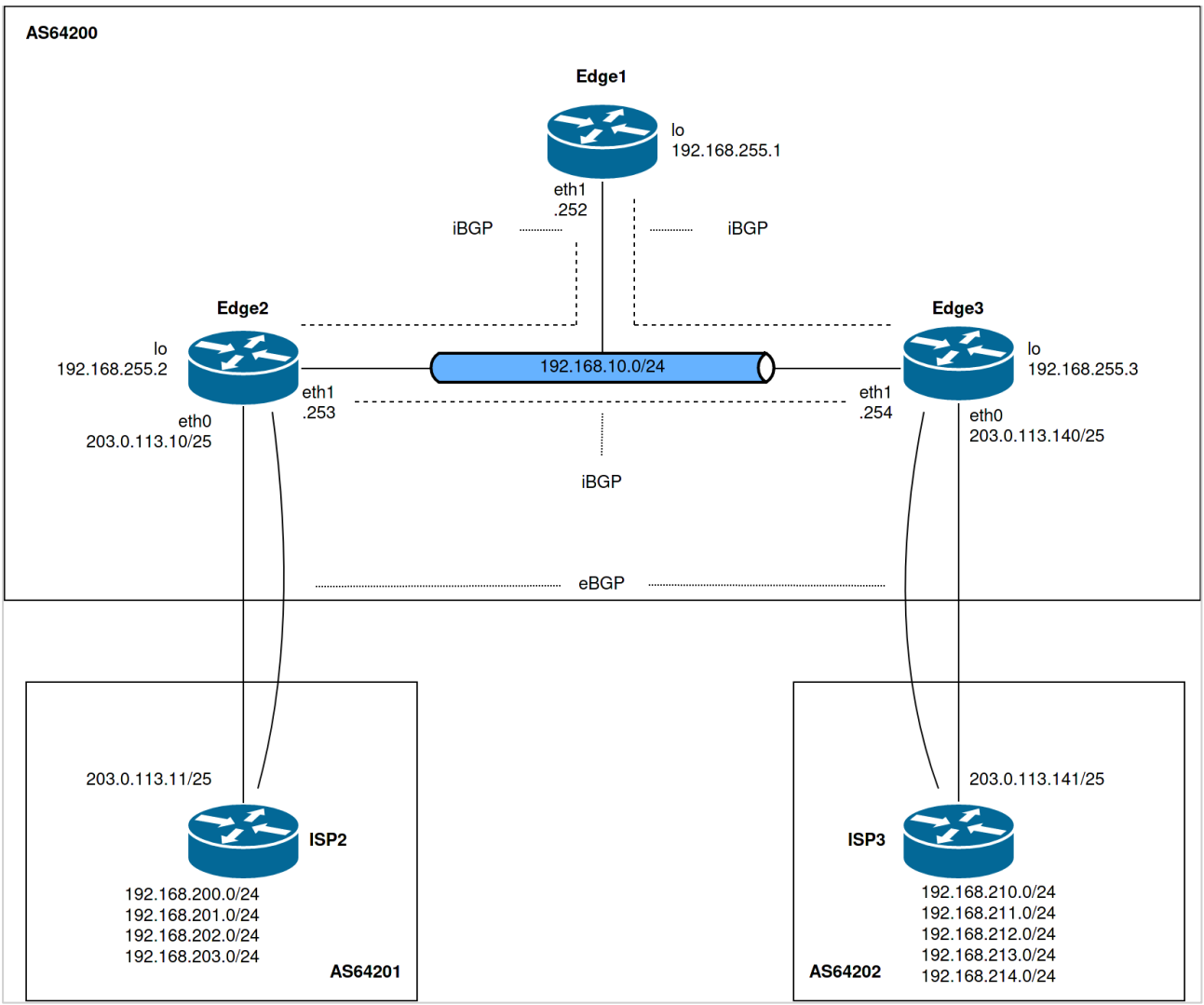


Рисунок 64 – Схема настройки BGP

В этой главе рассматриваются следующие вопросы:

- базовая конфигурация iBGP;
- проверка базовой конфигурации iBGP;
- базовая конфигурация eBGP;
- проверка конфигурации eBGP;
- создание маршрута для узла eBGP;
- проверка созданного маршрута;
- фильтрация входящих маршрутов;
- проверка фильтрации входящих маршрутов;
- фильтрация исходящих маршрутов;
- проверка фильтрации исходящих маршрутов;
- создание конфедерации BGP;
- проверка конфедерации BGP;
- отражатели маршрутов;
- проверка отражателя маршрутов;
- перенаправление маршрутов.

Базовая конфигурация iBGP

В данном примере рассматривается настройка iBGP на трех маршрутизаторах, обозначенных как Edge1, Edge2 и Edge3 на рисунке. Каждый маршрутизатор соединён посредством iBGP с каждым другим маршрутизатором (схема «каждый с каждым»).

Соединения iBGP установлены через IP-адреса, присвоенные интерфейсу заглушки (это обычная практика при наличии избыточных соединений между маршрутизаторами iBGP).

Каждый узел iBGP должен использовать внутренний протокол шлюза (Interior Gateway Protocol – IGP). В данном примере используется протокол OSPF для анонсирования адреса интерфейса заглушки внутри сети iBGP.

На рисунке показана базовая конфигурация iBGP.

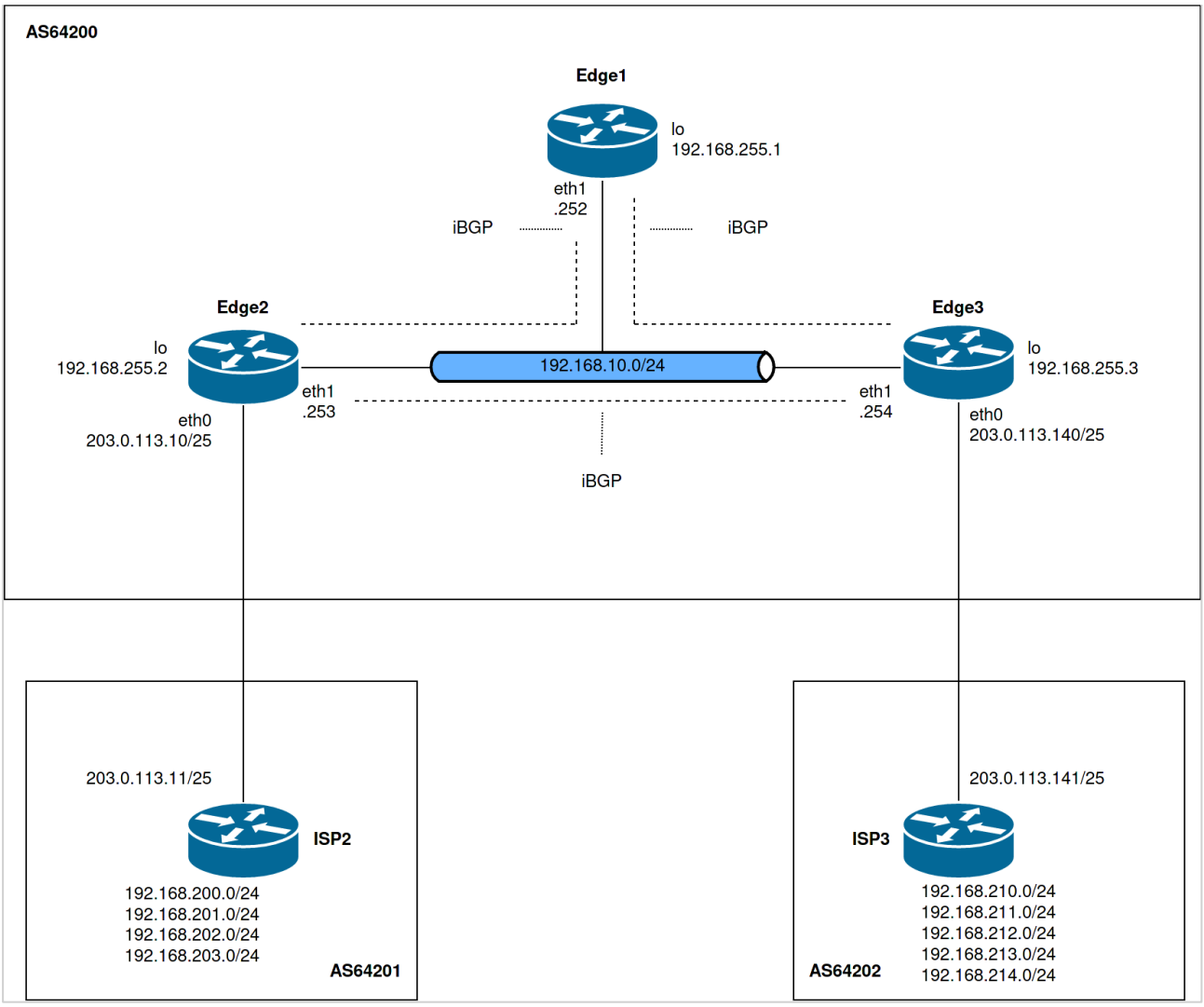


Рисунок 65 – Базовая конфигурация iBGP

В данном примере предполагается, что настройка интерфейсов маршрутизаторов уже выполнена.

Для настройки базовой конфигурации iBGP, соответствующей данному примеру, необходимо выполнить следующие действия:

Пример 243 – Базовая конфигурация iBGP.

Настройка Edge1		
Маршрутизатор	**Действие**	**Команда**
Edge1	Объявление для сети 192.168.255.1/32 в OSPF .	`[edit]` `admin@Edge1# set protocols ospf area 0.0.0.0 network 192.168.255.1/32`
Edge1	Объявление для сети 192.168.10.0/24 в OSPF.	`[edit]` `admin@Edge1# set protocols ospf area 0.0.0.0 network 192.168.10.0/24`
Edge1	Установка адреса интерфейса заглушки в	`[edit]`

	качестве идентификатора маршрутизатора в OSPF.	admin@Edge1# set protocols ospf parameters router-id 192.168.255.1
Edge1	Создание узла iBGP для маршрутизатора Edge2. Данный маршрутизатор является узлом iBGP, так как находится в той же АС, что и Edge1.	[edit] admin@Edge1# set protocols bgp 64200 neighbor 192.168.255.2 remote-as 64200
Edge1	Указание IP-адреса маршрутизатора Edge1 в качестве адреса получения обновлений маршрутной информации для маршрутизатора Edge2	[edit] admin@Edge1# set protocols bgp 64200 neighbor 192.168.255.2 update-source 192.168.255.1
Edge1	Создание узла iBGP для маршрутизатора Edge3. Данный маршрутизатор является узлом iBGP, так как находится в той же АС, что и Edge1.	[edit] admin@Edge1# set protocols bgp 64200 neighbor 192.168.255.3 remote-as 64200
Edge1	Указание IP-адреса маршрутизатора Edge1 в качестве адреса получения обновлений маршрутной информации для маршрутизатора Edge3.	[edit] admin@Edge1# set protocols bgp 64200 neighbor 192.168.255.3 update-source 192.168.255.1
Edge1	Указание IP-адреса интерфейса заглушки в качестве BGP-ID.	[edit] admin@Edge1# set protocols bgp 64200 parameters router-id 192.168.255.1
Edge1	Фиксация изменений.	[edit] admin@Edge1# commit

Edge1	Вывод настроек текущей конфигурации.	[edit]
		admin@Edge1# show protocols
		bgp 64200 {
		  neighbor 192.168.255.2 {
		  remote-as 64200
		  update-source 192.168.255.1
		  }
		  neighbor 192.168.255.3 {
		  remote-as 64200
		  update-source 192.168.255.1
		  }
		  parameters {
		  router-id 192.168.255.1
		  }
		}
		ospf {
		  area 0.0.0.0 {
		  network 192.168.255.1/32
		  network 192.168.10.0/24
		  }
		  parameters {
		  router-id 192.168.255.1
		  }
		}

Настройка маршрутизатора Edge2		
Маршрутизатор	**Действие**	**Команда**
Edge2	Объявление для сети 192.168.255.2/32 в OSPF.	[edit] admin@Edge2# set protocols ospf area 0.0.0.0 network 192.168.255.2/32
Edge2	Объявление для сети 192.168.10.0/24 в OSPF.	[edit] admin@Edge2# set protocols ospf area 0.0.0.0 network 192.168.10.0/24

Edge2	Объявление для сети 203.0.113.0/25 в OSPF.	[edit] admin@Edge2# set protocols ospf area 0.0.0.0 network 203.0.113.0/25
Edge2	Установка пассивного режима для интерфейса Ethernet **eth0** в OSPF.	[edit] admin@Edge2# set protocols ospf passive-interface eth0
Edge2	Установка адреса интерфейса заглушки в качестве идентификатора маршрутизатора в OSPF.	[edit] admin@Edge2# set protocols ospf parameters router-id 192.168.255.2
Edge2	Создание узла iBGP для маршрутизатора Edge1. Данный маршрутизатор является узлом iBGP, так как находится в той же АС, что и Edge2.	[edit] admin@Edge2# set protocols bgp 64200 neighbor 192.168.255.1 remote-as 64200
Edge2	Указание IP-адреса маршрутизатора Edge2 в качестве адреса получения обновлений маршрутной информации для маршрутизатора Edge1.	[edit] admin@Edge2# set protocols bgp 64200 neighbor 192.168.255.1 update-source 192.168.255.2
Edge2	Создание узла iBGP для маршрутизатора Edge3. Данный маршрутизатор является узлом iBGP, так как находится в той же АС, что и Edge2.	[edit] admin@Edge2# set protocols bgp 64200 neighbor 192.168.255.3 remote-as 64200
Edge2	Указание IP-адреса маршрутизатора Edge2 в качестве адреса получения обновлений маршрутной информации для маршрутизатора Edge3.	[edit] admin@Edge2# set protocols bgp 64200 neighbor 192.168.255.3 update-source 192.168.255.2
Edge2	Указание IP-адреса интерфейса заглушки в качестве BGP-ID.	[edit] admin@Edge2# set protocols bgp 64200 parameters router-id 192.168.255.2
Edge2	Фиксация изменений.	[edit] admin@Edge2# commit

Edge2	Вывод настроек текущей конфигурации.	[edit]
		admin@Edge2# show protocols
		bgp 64200 {
		  neighbor 192.168.255.1 {
		  remote-as 64200
		  update-source 192.168.255.2
		  }
		  neighbor 192.168.255.3 {
		  remote-as 64200
		  update-source 192.168.255.2
		  }
		  parameters {
		  router-id 192.168.255.2
		  }
		}
		ospf {
		  area 0.0.0.0 {
		  network 192.168.255.2/32
		  network 192.168.10.0/24
		  network 203.0.113.0/25
		  }
		  parameters {
		  router-id 192.168.255.2
		  }
		  passive-interface eth0
		}

Настройка Edge3		

Маршрутизатор	Действие	Команда
Edge3	Объявление для сети 192.168.255.3/32 в OSPF.	[edit] admin@Edge3# set protocols ospf area 0.0.0.0 network 192.168.255.3/32
Edge3	Объявление для сети 192.168.10.0/24 в OSPF.	[edit] admin@Edge3# set protocols ospf area 0.0.0.0 network 192.168.10.0/24
Edge3	Объявление для сети 203.0.113.128/25 в OSPF.	[edit] admin@Edge3# set protocols ospf area 0.0.0.0 network 203.0.113.128/25
Edge3	Установка адреса интерфейса заглушки в качестве идентификатора маршрутизатора в OSPF.	[edit] admin@Edge3# set protocols ospf parameters router-id 192.168.255.3
Edge3	Установка пассивного режима для интерфейса Ethernet **eth0** в OSPF.	[edit] admin@Edge3# set protocols ospf passive-interface eth0
Edge3	Создание узла iBGP для маршрутизатора Edge1. Данный маршрутизатор является узлом iBGP, так как находится в той же AC, что и Edge3.	[edit] admin@Edge3# set protocols bgp 64200 neighbor 192.168.255.1 remote-as 64200
Edge3	Указание IP-адреса маршрутизатора Edge3 в качестве адреса получения обновлений маршрутной информации для маршрутизатора Edge1.	[edit] admin@Edge3# set protocols bgp 64200 neighbor 192.168.255.1 update-source 192.168.255.3
Edge3	Создание узла iBGP для маршрутизатора Edge2. Данный маршрутизатор является узлом iBGP, так как находится в той же AC, что и Edge3.	[edit] admin@Edge3# set protocols bgp 64200 neighbor 192.168.255.2 remote-as 64200
Edge3	Указание IP-адреса маршрутизатора Edge3 в качестве адреса получения обновлений маршрутной информации для маршрутизатора Edge2.	[edit] admin@Edge3# set protocols bgp 64200 neighbor 192.168.255.2 update-source 192.168.255.3
Edge3	Указание IP-адреса интерфейса заглушки в качестве BGP-ID.	[edit] admin@Edge3# set protocols bgp 64200 parameters router-id 192.168.255.3
Edge3	Фиксация изменений.	[edit] admin@Edge3# commit

Edge3	Вывод настроек текущей конфигурации.	[edit]
		admin@Edge3# show protocols
		bgp 64200 {
		  neighbor 192.168.255.1 {
		  remote-as 64200
		  update-source 192.168.255.3
		  }
		  neighbor 192.168.255.2 {
		  remote-as 64200
		  update-source 192.168.255.3
		  }
		  parameters {
		  router-id 192.168.255.3
		  }
		}
		ospf {
		  area 0.0.0.0 {

		network 192.168.255.3/32
		network 192.168.10.0/32
		network 203.0.113.128/25
		}
		parameters {
		router-id 192.168.255.3
		}
		passive-interface eth0
		}

Проверка базовой конфигурации iBGP

Для проверки текущей конфигурации iBGP используются следующие команды, выполняемые в эксплуатационном режиме: **show ip bgp summary** и **show ip bgp**. Обе команды выполняются на маршрутизаторе Edge1.

В примере ниже показан вывод команды **show ip bgp summary** на маршрутизаторе Edge1.

Пример 244 – Проверка базовой конфигурации iBGP на маршрутизаторе Edge1: вывод кратких сведений о состоянии соединения BGP.

```
admin@Edge1:~$ show ip bgp summary
BGP router identifier 192.168.255.1, local AS number 64200
RIB entries 0, using 0 bytes of memory
Peers 2, using 18 KiB of memory

Neighbor      V       AS MsgRcvd MsgSent OutQ  Up/Down  State        PfxRcd
192.168.255.2 4    64200       6       7    0  00:00:13 Established       0
192.168.255.3 4    64200       7       8    0  00:00:02 Established       0

Total number of neighbors 2

Total num. Established sessions 2
Total num. of routes received 0
```

Значения Up/Down показывает время работы/простоя узла iBGP. Значение State равное Established означает, что узел успешно установил соединение со своим BGP соседом и способен производить обмен объявлениями об изменении маршрутной информации.

В примере ниже показан вывод команды **show ip bgp** на маршрутизаторе Edge1.

Пример 245 – Проверка базовой конфигурации iBGP на маршрутизаторе Edge1: вывод сведений о составе таблицы маршрутизации BGP

```
admin@Edge1:~$ show ip bgp

No BGP prefixes displayed, 0 exist
```

Данный пример показывает, что таблица маршрутизации BGP не содержит каких-либо маршрутов, по причине того, что анонс марштуров внутри данной AS не был настроен ни на одном маршрутизаторе.

Базовая конфигурация eBGP

В данном разделе рассматривается настройка eBGP на маршрутизаторах Edge2 и Edge3, а также на IPS2 и IPS3 как показано на рисунке ниже. Маршрутизатор Edge2 соединен с узлом IPS2, состоящим в AC номер 64201, маршрутизатор Edge3 соединен с узлом IPS3, состоящем в AC номер 64202.

В данном примере, соединения eBGP установлены между узлами eBGP с использованием физического IP-адреса интерфейса. При этом отсутствует избыточность соединений (при сбое в одном из маршрутизаторов, пиринг между AC осуществляться не будет).

На рисунке показана базовая конфигурация eBGP.

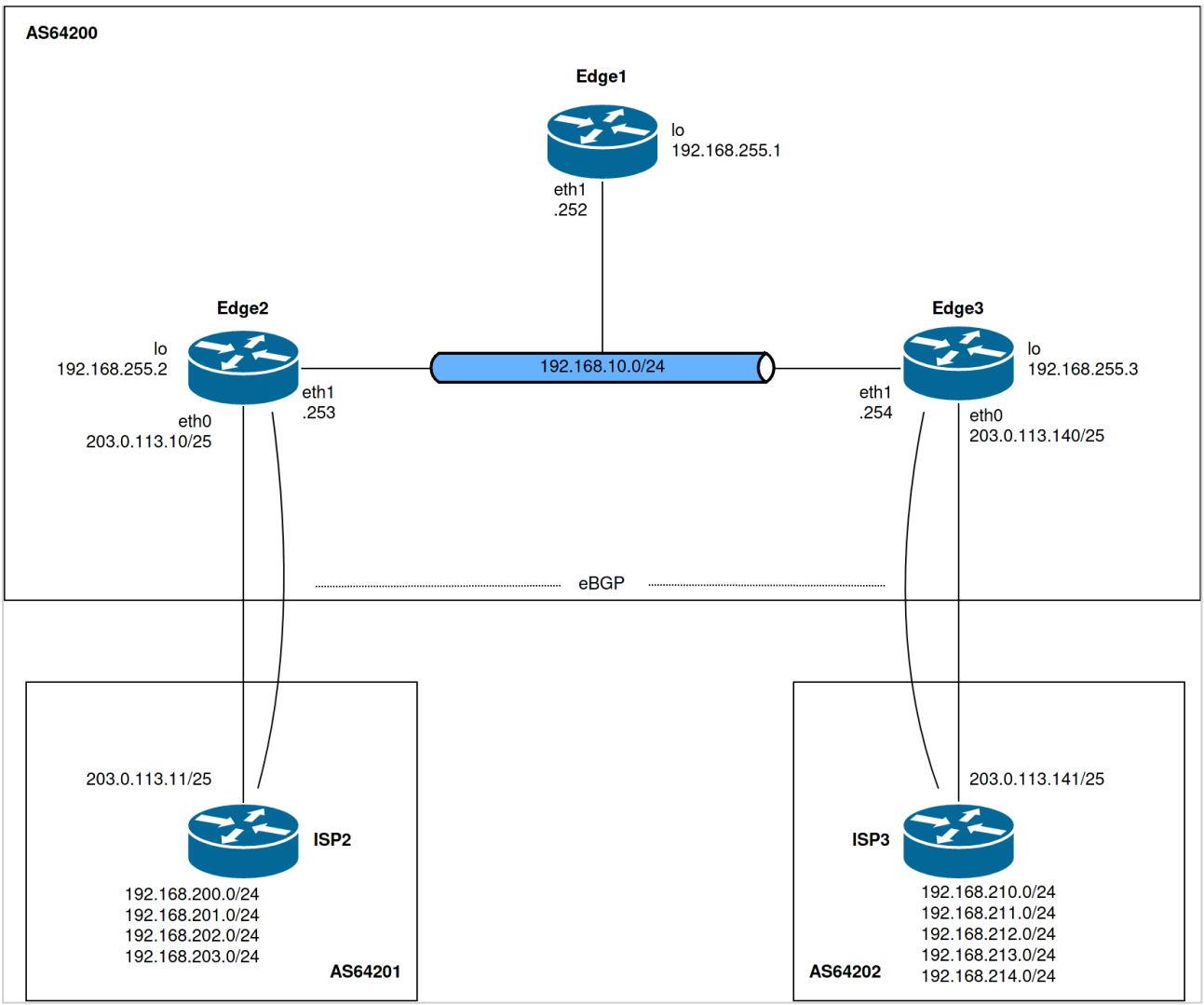


Рисунок 66 – Базовая конфигурация eBGP

Для настройки базовой конфигурации eBGP, соответствующей данному примеру, необходимо выполнить следующие действия:

Пример 246 – Базовая конфигурация eBGP.

Настройка Edge2		
Маршрутизатор	**Действие**	**Команда**
Edge2	Указание адреса узла eBGP для маршрутизатора Edge2.	`[edit]` `admin@Edge2# set protocols bgp 64200 neighbor 203.0.113.11 remote-as 64201`
Edge2	Фиксация изменений.	`[edit]` `admin@Edge2# commit`
Настройка ISP2		
ISP2	Указание адреса узла eBGP для маршрутизатора ISP2.	`[edit]` `admin@IPS2# set protocols bgp 64201 neighbor 203.0.113.10 remote-as 64200`
ISP2	Указание IP-адреса, BGP соседа в качестве BGP-ID.	`[edit]` `admin@IPS2# set protocols bgp 64201 parameters router-id 203.0.113.10`
ISP2	Объявление подсети 192.168.200.0/24 для автономной системы 64201.	`[edit]` `admin@IPS2# set protocols bgp 64201 network 192.168.200.0/24`

ISP2	Объявление подсети 192.168.201.0/24 для автономной системы 64201.	[edit] admin@IPS2# set protocols bgp 64201 network 192.168.201.0/24
ISP2	Объявление подсети 192.168.202.0/24 для автономной системы 64201.	[edit] admin@IPS2# set protocols bgp 64201 network 192.168.202.0/24
ISP2	Объявление подсети 192.168.203.0/24 для автономной системы 64201.	[edit] admin@IPS2# set protocols bgp 64201 network 192.168.203.0/24
ISP2	Фиксация изменений.	[edit] admin@IPS2# commit
Настройка Edge3		
Edge3	Указание адреса узла eBGP для маршрутизатора Edge2.	[edit] admin@Edge3# set protocols bgp 64200 neighbor 203.0.113.141 remote-as 64202
Edge3	Фиксация изменений.	[edit] admin@Edge3# commit
Настройка ISP3		
ISP3	Указание адреса узла eBGP для маршрутизатора ISP3.	[edit] admin@IPS2# set protocols bgp 642012 neighbor 203.0.113.140 remote-as 64200
ISP3	Указание IP-адреса, BGP соседа в качестве BGP-ID.	[edit] admin@IPS2# set protocols bgp 64202 parameters router-id 203.0.113.141
ISP3	Объявление подсети 192.168.210.0/24 для автономной системы 64202.	[edit] admin@IPS2# set protocols bgp 64202 network 192.168.210.0/24
ISP3	Объявление подсети 192.168.211.0/24 для автономной системы 64202.	[edit] admin@IPS2# set protocols bgp 64202 network 192.168.211.0/24
ISP3	Объявление подсети 192.168.212.0/24 для автономной системы 64202.	[edit] admin@IPS2# set protocols bgp 64202 network 192.168.212.0/24
ISP3	Объявление подсети 192.168.213.0/24 для автономной системы 64202.	[edit] admin@IPS2# set protocols bgp 64202 network 192.168.213.0/24
ISP3	Объявление подсети 192.168.214.0/24 для автономной системы 64202.	[edit] admin@IPS2# set protocols bgp 64202 network 192.168.214.0/24
ISP3	Фиксация изменений.	[edit] admin@IPS2# commit

Проверка базовой конфигурации eBGP

Для проверки текущей конфигурации eBGP используются следующие команды, выполняемые в эксплуатационном режиме: **show ip bgp summary** и **show ip bgp**. Обе команды выполняются на маршрутизаторе Edge2.

В примере ниже показан вывод команды **show ip bgp summary** на маршрутизаторе Edge2.

Пример 247 – Проверка базовой конфигурации eBGP на маршрутизаторе Edge2: вывод кратких сведений о состоянии соединения BGP.

```
admin@Edge2:~$ show ip bgp summary
BGP router identifier 192.168.255.2, local AS number 64200
RIB entries 17, using 1904 bytes of memory
Peers 3, using 27 KiB of memory

Neighbor      V AS    MsgRcvd MsgSent OutQ Up/Down   State        PfxRcd
192.168.255.1 4 64200 6       8        0    00:02:54  Established  0
192.168.255.3 4 64200 5       7        0    00:02:41  Established  0
203.0.113.11  4 64201 4       5        0    00:00:25  Established  0

Total number of neighbors 3

Total num. Established sessions 3
Total num. of routes received 9
```

После добавления узла eBGP с адресом 203.0.113.11, можно увидеть время соединения с данным узлом в соответствующем поле Up/Down. А состояние Established говорит о том, что данный узел имеет правильные настройки, так как между ним и маршрутизатором Edge2 успешно установлено соединение.

Значение полей MsgRcvd и MsgSent для данного узла с адресом 203.0.113.11 означают, что узел получил 4 сообщений и отправил 5 сообщений BGP.

Значение 0 в столбце PfxRcd означает, что маршрутизатор Edge2 не получал префиксов от iBGP узла с адресом 192.168.255.1.

От маршрутизатора 192.168.255.3 было получено 5 префиксов, которые тот в свою очередь получил по eBGP от маршрутизатора 203.0.113.141. Узнаазать список полученных префиксов от опредлененного BGP соседа можно командой **show ip bgp ipv4 unicast neighbors 192.168.255.3 routes.**

Пример 248 – Просмотр префиксов, анонсируемых iBGP соседом Edge3.

```
admin@Edge2:~$ show ip bgp ipv4 unicast neighbors 192.168.255.3 routes
BGP table version is 0, local router ID is 192.168.255.2
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i192.168.210.0    203.0.113.141            0    100      0 64202 i
*>i192.168.211.0    203.0.113.141            0    100      0 64202 i
*>i192.168.212.0    203.0.113.141            0    100      0 64202 i
*>i192.168.213.0    203.0.113.141            0    100      0 64202 i
*>i192.168.214.0    203.0.113.141            0    100      0 64202 i

Displayed  5 out of 9 total prefixes
```

Для просмотра префиксов, полученных по eBGP от маршрутизатора 203.0.113.11 воспользуйтесь аналогичной командой.

Пример 249 – Просмотр префиксов, анонсируемых eBGP соседом IPS2

```
admin@Edge2:~$ show ip bgp ipv4 unicast neighbors 203.0.113.11 routes
BGP table version is 0, local router ID is 192.168.255.2
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.200.0    203.0.113.11             0             0 64201 i
*> 192.168.201.0    203.0.113.11             0             0 64201 i
*> 192.168.202.0    203.0.113.11             0             0 64201 i
*> 192.168.203.0    203.0.113.11             0             0 64201 i

Displayed  4 out of 9 total prefixes
admin@edge01:~$
```

В примере ниже показан вывод команды show ip bgp на маршрутизаторе Edge2.

Пример 250 – Проверка базовой конфигурации eBGP на маршрутизаторе Edge2: вывод сведений о составе таблицы маршрутизации BGP

```
admin@Edge2:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.255.2
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.200.0    203.0.113.11             0             0 64201 i
*> 192.168.201.0    203.0.113.11             0             0 64201 i
*> 192.168.202.0    203.0.113.11             0             0 64201 i
*> 192.168.203.0    203.0.113.11             0             0 64201 i
*>i192.168.210.0    203.0.113.141            0    100      0 64202 i
*>i192.168.211.0    203.0.113.141            0    100      0 64202 i
*>i192.168.212.0    203.0.113.141            0    100      0 64202 i
*>i192.168.213.0    203.0.113.141            0    100      0 64202 i
*>i192.168.214.0    203.0.113.141            0    100      0 64202 i

Displayed  9 out of 9 total prefixes
```

Создание маршрута для узла eBGP.

Одним из основных требований BGP является создание префикса сети с последующим анонсированием для узлов BGP. В Numa Edge данное условие реализуется посредством настройки сети в рамках конфигурации BGP.

В данном разделе рассматривается создание префикса сети и его последующее анонсирование для маршрутизаторов Edge2 и Edge3, как показано на рисунке ниже.

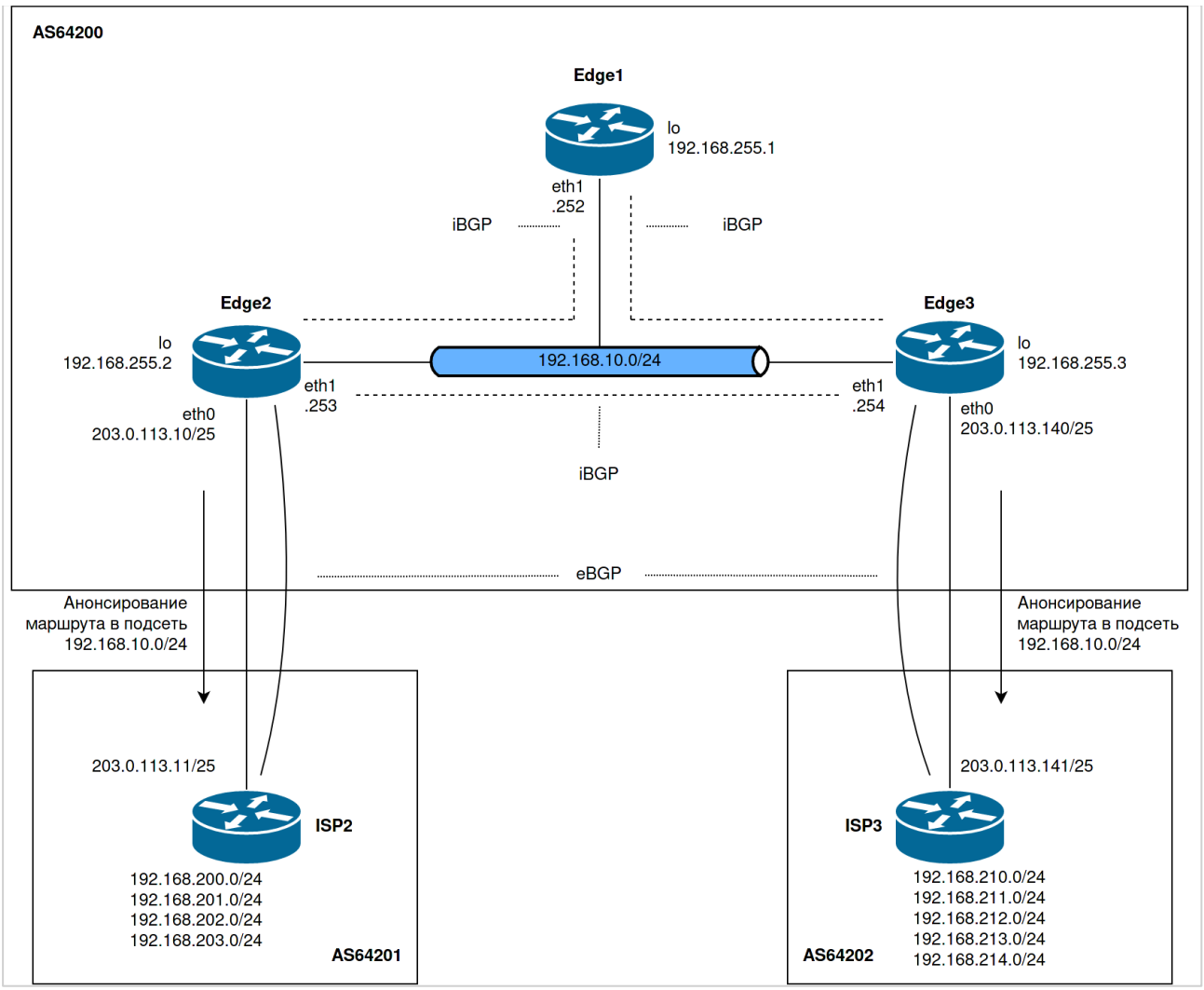


Рисунок 67 – Создание маршрута для узла eBGP

В данном примере предполагается, что выполнены все настройки, описанные в предыдущих разделах.

Для создания и последующего анонсирования маршрута для узла eBGP, необходимо выполнить следующие действия:

Пример 251 – Создание маршрута для узла eBGP

Настройка маршрутизатора Edge2		
Маршрутизатор	**Действие**	**Команда**
Edge2	Объявление локальной сети для сети BGP.	`[edit]` `admin@Edge2# set protocols bgp 64200 network 192.168.10.0/24`
Edge2	Фиксация изменений.	`[edit]` `admin@Edge2# commit`
Настройка маршрутизатора Edge3		
Edge3	Объявление локальной сети для сети BGP.	`[edit]` `admin@Edge3# set protocols bgp 64200 network 192.168.10.0/24`
Edge3	Фиксация изменений.	`[edit]` `admin@Edge3# commit`

Проверка созданного маршрута

Для проверки созданного маршрута используются следующие команды, выполняемые в эксплуатационном режиме: show ip bgp summary и show ip bgp. Обе команды выполняются на маршрутизаторе Edge2. Значение в столбце MsgSent показывает количество BGP сообщений, отправленных маршрутизатором для каждого узла.

В примере ниже показан вывод команды **show ip bgp summary** на маршрутизаторе Edge2.

Пример 252 – Проверка созданного маршрута на маршрутизаторе Edge2: вывод кратких сведений о состоянии соединения BGP

```
admin@Edge2:~$ show ip bgp
summary  BGP router identifier 192.168.255.2, local AS number 64200
RIB entries 19, using 2128 bytes of memory
Peers 3, using 27 KiB of memory

Neighbor        V    AS MsgRcvd MsgSent OutQ Up/Down  State         PfxRcd
192.168.255.1   4 64200      84      87    0 01:20:16 Established        0
192.168.255.3   4 64200      84      86    0 01:20:03 Established        6
203.0.113.11    4 64201      81      83    0 01:17:47 Established        4

Total number of neighbors 3

Total num. Established sessions 3
Total num. of routes received     10
```

Значения, показанные в столбце PfxRcd означают, что маршрутизатор Edge2 получил 6 префиксов от узла с IP-адресом 192.168.255.3 и 4 префикса от узла с IP-адресом 203.0.113.11.

В примере ниже показан вывод команды **show ip bgp** на маршрутизаторе Edge2.

Пример 253 – Проверка созданного маршрута на маршрутизаторе Edge2: вывод сведений о составе таблицы маршрутизации BGP

```
admin@Edge2:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.255.2
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
* i192.168.10.0     192.168.255.3            0    100      0 i
*>                  0.0.0.0                  0         32768 i
*> 192.168.200.0    203.0.113.11             0             0 64201 i
*> 192.168.201.0    203.0.113.11             0             0 64201 i
*> 192.168.202.0    203.0.113.11             0             0 64201 i
*> 192.168.203.0    203.0.113.11             0             0 64201 i
*>i192.168.210.0    203.0.113.141            0    100      0 64202 i
*>i192.168.211.0    203.0.113.141            0    100      0 64202 i
*>i192.168.212.0    203.0.113.141            0    100      0 64202 i
*>i192.168.213.0    203.0.113.141            0    100      0 64202 i
*>i192.168.214.0    203.0.113.141            0    100      0 64202 i
Displayed  10 out of 11 total prefixes
```

Данный пример показывает, что таблица маршрутизации BGP содержит 9 префиксов: 4 из АС номер 64201 и 5 из АС номер 64202.

Символ «*» в начале показывает статус данного маршрута (то, что этот маршрут действителен). Символ «>» показывает, что данный путь выбран «лучшим» процессом выбора наилучшего пути BGP. Команда show ip bgp показывает только те пути, которые были выбраны «лучшими».

В примере ниже показан вывод команды **show ip route bgp** на маршрутизаторе Edge2.

Пример 254 – Проверка созданного маршрута на маршрутизаторе Edge2: вывод таблицы маршрутизации BGP

```
admin@Edge2:~$ show ip route bgp
Codes: K - kernel route, C - connected, S - static, R - RIP,
O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
> - selected route, * - FIB route

B>* 192.168.200.0/24 [20/0] via 203.0.113.11, eth0, 00:11:48
B>* 192.168.201.0/24 [20/0] via 203.0.113.11, eth0, 00:11:48
B>* 192.168.202.0/24 [20/0] via 203.0.113.11, eth0, 00:11:48
B>* 192.168.203.0/24 [20/0] via 203.0.113.11, eth0, 00:11:48
B>  192.168.210.0/24 [200/0] via 203.0.113.141 (recursive), 00:10:34
*                           via 192.168.10.254, eth1, 00:10:34
B>  192.168.211.0/24 [200/0] via 203.0.113.141 (recursive), 00:10:34
*                           via 192.168.10.254, eth1, 00:10:34
B>  192.168.212.0/24 [200/0] via 203.0.113.141 (recursive), 00:10:34
*                           via 192.168.10.254, eth1, 00:10:34
B>  192.168.213.0/24 [200/0] via 203.0.113.141 (recursive), 00:10:34
*                           via 192.168.10.254, eth1, 00:10:34
B>  192.168.214.0/24 [200/0] via 203.0.113.141 (recursive), 00:10:34
*                           via 192.168.10.254, eth1, 00:10:34
```

Вывод данной команды показывает только те маршруты BGP, которые прописаны в базе маршрутной информации (RIB). Вывод этой команды на маршрутизаторе Edge2 соответствует выводу на маршрутизаторе Edge3.

В примере ниже показан вывод команды **show ip bgp summary** на маршрутизаторе Edge3.

Пример 255 – Проверка созданного маршрута на маршрутизаторе Edge3: вывод кратких сведений о состоянии соединения BGP

```
admin@Edge3:~$ show ip bgp summary
BGP router identifier 192.168.255.3, local AS number 64200
RIB entries 19, using 2128 bytes of memory
Peers 3, using 27 KiB of memory

Neighbor        V    AS MsgRcvd MsgSent OutQ Up/Down  State         PfxRcd
192.168.255.1   4 64200      89      92    0 01:24:20 Established        0
192.168.255.2   4 64200      89      90    0 01:24:28 Established        5
203.0.113.141   4 64202      85      88    0 01:21:59 Established        5

Total number of neighbors 3

Total num. Established sessions 3
Total num. of routes received     10
```

В примере ниже показан вывод команды **show ip bgp** на маршрутизаторе Edge3.

Пример 256 – Проверка созданного маршрута на маршрутизаторе Edge3: вывод сведений о составе таблицы маршрутизации BGP

```
admin@Edge3:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.255.3
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network       Next Hop      Metric LocPrf Weight  Path
*>  192.168.10.0  0.0.0.0       0              32768   i
* i               192.168.255.2 0      100     0       i
*>i 192.168.200.0 203.0.113.11  0      100     0       64201 i
*>i 192.168.201.0 203.0.113.11  0      100     0       64201 i
*>i 192.168.202.0 203.0.113.11  0      100     0       64201 i
*>i 192.168.203.0 203.0.113.11  0      100     0       64201 i
*>  192.168.210.0 203.0.113.141 0              0       64202 i
*>  192.168.211.0 203.0.113.141 0              0       64202 i
*>  192.168.212.0 203.0.113.141 0              0       64202 i
*>  192.168.213.0 203.0.113.141 0              0       64202 i
*>  192.168.214.0 203.0.113.141 0              0       64202 i
```

Таблица BGP маршрутизатора Edge3 содержит пути, полученные как от узлов eBGP, так и от узла iBGP, в качестве которого выступает маршрутизатор Edge2.

Фильтрация входящих маршрутов.

Одним из главных требований при реализации BGP является фильтрация определённых входящих анонсов маршрутов от узлов BGP. В Numa edge данное требование реализовано посредством использования определённых политик маршрутизации, применяемых к процессу BGP в качестве политики импорта. При создании политики используется связка карты маршрутов и списка префиксов.

На рисунке показано применение политики фильтрации входящих маршрутов, в которой маршрутизатор Edge2 принимает от узла eBGP только маршруты к подсетям 192.168.200.0/24 и 192.168.202.0/24 и отвергает все остальные маршруты, а маршрутизатор Edge3 принимает все маршруты, кроме маршрутов к подсетям 192.168.210.0/24 и 192.168.213.0/24.

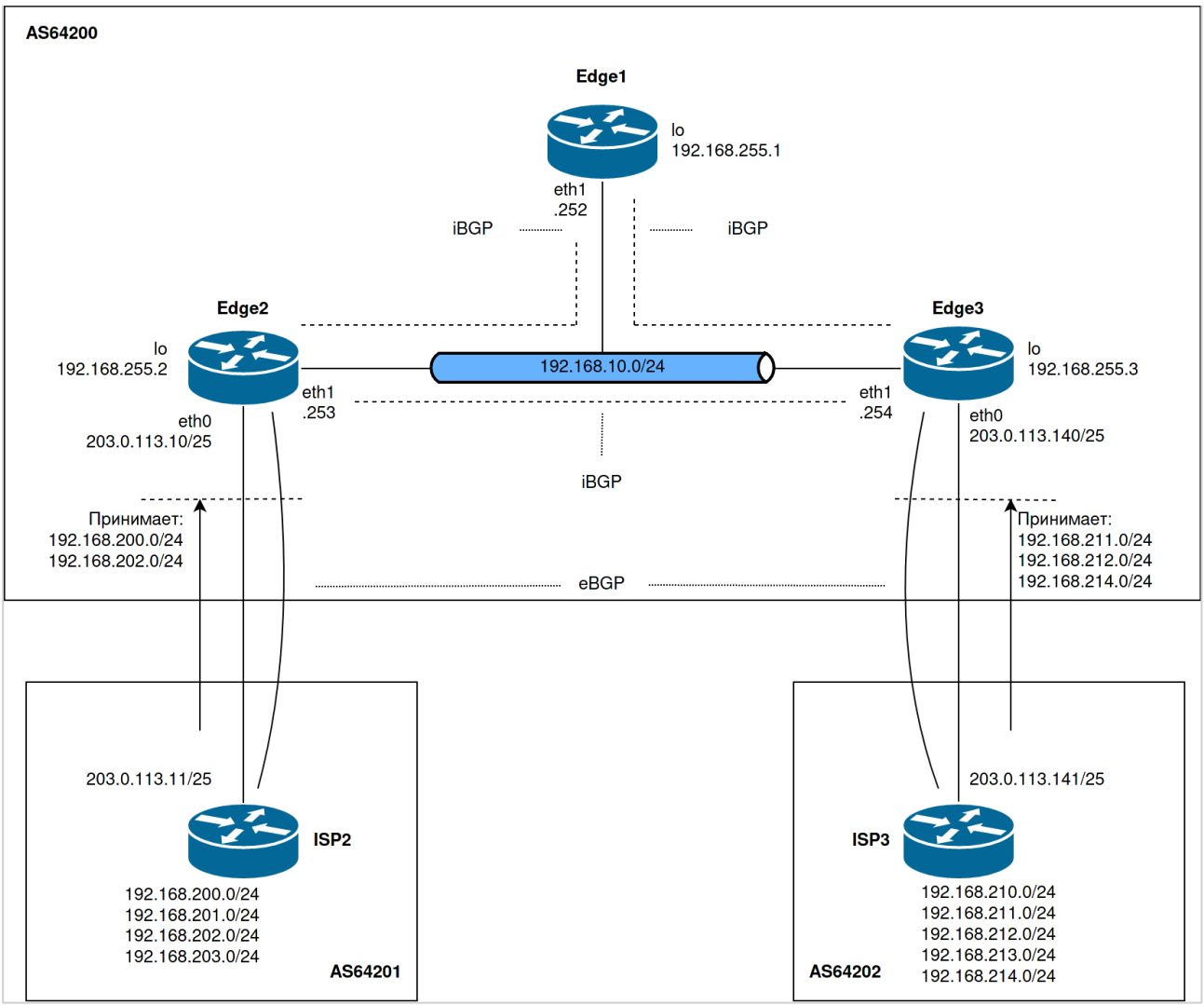


Рисунок 68 – Фильтрация входящих маршрутов

Для настройки фильтрации входящих маршрутов необходимо выполнить следующие действия:

Пример 257 – Фильтрация входящих маршрутов

Настройка маршрутизатора Edge2		
Маршрутизатор	**Действие**	**Команда**

Edge2	Создание правила соответствия всем префиксу 192.168.200.0/24.	`[edit]`
		`admin@Edge2# set policy prefix-list Allow-Prefix rule 1 action permit`
		`[edit]`
		`admin@Edge2# set policy prefix-list Allow-Prefix rule 1 prefix 192.168.200.0/24`

Edge2	Создание правила соответствия всем префиксу 192.168.202.0/24.	`[edit]`
		`admin@Edge2# set policy prefix-list Allow-Prefix rule 2 action permit`
		`[edit]`
		`admin@Edge2# set policy prefix-list Allow-Prefix rule 2 prefix 192.168.202.0/24`

Edge2	Создание карты маршрутов. Указание правила разрешения префиксов, указанных в списке Allow-Prefix.	[edit] admin@Edge2# set policy route-map eBGP-Import-route rule 10 action permit [edit] admin@Edge2# set policy route-map eBGP-Import-route rule 10 match ip address prefix-list Allow-Prefix
Edge2	Создание правила запрета всех остальных маршрутов в рамках указанной карты маршрутов.	[edit] admin@Edge2# set policy route-map eBGP-Import-route rule 20 action deny
Edge2	Применение созданной карты маршрутов в качестве политики импорта для АС с номером 64201.	[edit] admin@Edge2# set protocols bgp 64200 neighbor 203.0.113.11 route-map import eBGP-Import-route
Edge2	Фиксация изменений.	[edit] admin@Edge2# commit
Edge2	Сброс текущей сессии BGP для узла с адресом 203.0.113.11 (для применения созданной политики).	[edit] admin@Edge2# run clear ip bgp 203.0.113.11

Edge2	Вывод настроек текущей конфигурации.	[edit]
		admin@Edge2# show policy
		prefix-list Allow-Prefix {
		rule 1 {
		action permit
		prefix 192.168.200.0/24
		}
		rule 2 {
		action permit
		prefix 192.168.202.0/24
		}
		}
		route-map eBGP-Import-route {
		rule 10 {
		action permit
		match {
		ip {
		address {
		prefix-list Allow-Prefix
		}
		}
		}
		}
		rule 20 {
		action deny
		}
		}

Edge2	Отображение конфигурации BGP для узла eBGP с IP-адресом 203.0.113.11.	[edit]
		admin@Edge2# show protocols bgp 64200 neighbor 203.0.113.11
		remote-as 64201
		route-map {
		import eBGP-Import-route
		}

Настройка маршрутизатора Edge3		
Edge3	Создание правила соответствия всем префиксу 192.168.210.0/24.	[edit] admin@Edge3# set policy prefix-list Allow-Prefix rule 1 action permit

Настройка маршрутизатора Edge3		
		[edit] admin@Edge3# set policy prefix-list Allow-Prefix rule 1 prefix 192.168.210.0/24
Edge3	Создание правила соответствия всем префиксу 192.168.213.0/24.	[edit] admin@Edge3# set policy prefix-list Allow-Prefix rule 2 action permit [edit] admin@Edge3# set policy prefix-list Allow-Prefix rule 2 prefix 192.168.213.0/24
Edge3	Создание карты маршрутов. Указание правила разрешения префиксов, указанных в списке Allow-Prefix.	[edit] admin@Edge3# set policy route-map eBGP-Import-route rule 10 action deny [edit] admin@Edge3# set policy route-map eBGP-Import-route rule 10 match ip address prefix-list Allow-Prefix
Edge3	Создание правила разрешения всех остальных префиксов в рамках указанной карты маршрутов.	[edit] admin@Edge3# set policy route-map eBGP-Import-route rule 20 action permit
Edge3	Применение созданной карты маршрутов в качестве политики импорта для АС с номером 64202.	[edit] admin@Edge3# set protocols bgp 64200 neighbor 203.0.113.141 route-map import eBGP-Import-route
Edge3	Фиксация изменений.	[edit] admin@Edge3# commit
Edge3	Сброс текущей сессии BGP для узла с адресом 203.0.113.141 (для применения созданной политики).	[edit] admin@Edge3# run clear ip bgp 203.0.113.141

Edge3	Вывод настроек текущей конфигурации.	[edit]
		admin@Edge3# show policy
		prefix-list Allow-Prefix {
		rule 1 {
		action permit
		prefix 192.168.210.0/24
		}
		rule 2 {
		action permit
		prefix 192.168.213.0/24
		}
		}
		route-map eBGP-Import-route {
		rule 10 {
		action deny
		match {
		ip {
		address {
		prefix-list Allow-Prefix
		}
		}
		}
		}
		rule 20 {
		action permit
		}
		}

Edge3	Отображение конфигурации BGP для	[edit]

Настройка маршрутизатора Edge3		

	узла eBGP с IP-адресом 203.0.113.141.	admin@Edge3# show protocols bgp 64200
		neighbor 203.0.113.141
		remote-as 64202
		route-map {
		import eBGP-Import-route
		}

Проверка фильтрации входящих маршрутов

В примере ниже показан вывод команды **show ip bgp** на маршрутизаторе Edge2 до применения политик импорта как на маршрутизаторе Edge2, так и на Edge3.

Пример 258 – Входящие маршруты BGP на маршрутизаторе Edge2 до применения политики импорта

```
admin@Edge2:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.255.2
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network      Next Hop      Metric LocPrf Weight Path
* i 192.168.10.0  192.168.255.3 0      100    0      i
*>                0.0.0.0       0              32768  i
*>  192.168.200.0 203.0.113.11  0              0      64201 i
*>  192.168.201.0 203.0.113.11  0              0      64201 i
*>  192.168.202.0 203.0.113.11  0              0      64201 i
*>  192.168.203.0 203.0.113.11  0              0      64201 i
*>i 192.168.210.0 203.0.113.141 0      100    0      64202 i
*>i 192.168.211.0 203.0.113.141 0      100    0      64202 i
*>i 192.168.212.0 203.0.113.141 0      100    0      64202 i
*>i 192.168.213.0 203.0.113.141 0      100    0      64202 i
*>i 192.168.214.0 203.0.113.141 0      100    0      64202 i
```

В примере ниже показан вывод команды **show ip bgp** на маршрутизаторе Edge2 после применения на нем политики импорта.

Пример 259 – Входящие маршруты BGP на маршрутизаторе Edge2 после применения политики импорта на данном маршрутизаторе

```
admin@Edge2:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.255.2
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network       Next Hop      Metric LocPrf Weight Path
* i 192.168.10.0  192.168.255.3 0      100    0      i
*>                0.0.0.0       0              32768  i
*>  192.168.200.0 203.0.113.11  0              0      64201 i
*>  192.168.202.0 203.0.113.11  0              0      64201 i
*>i 192.168.210.0 203.0.113.141 0      100    0      64202 i
*>i 192.168.211.0 203.0.113.141 0      100    0      64202 i
*>i 192.168.212.0 203.0.113.141 0      100    0      64202 i
*>i 192.168.213.0 203.0.113.141 0      100    0      64202 i
*>i 192.168.214.0 203.0.113.141 0      100    0      64202 i
```

Следует отметить, что от узла с адресом 203.0.113.11 в таблице остались только префиксы 192.168.200.0 и 192.168.202.0.

В примере ниже показан вывод команды **show ip bgp** на маршрутизаторе Edge3 после применения политик на Edge2, но до применения политики импорта на нем самом.

Пример 260 – Входящие маршруты BGP на маршрутизаторе Edge3 после применения политик на Edge2, но до применения политики импорта на нем самом

```
admin@Edge3:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.255.3
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network       Next Hop      Metric LocPrf Weight Path
*>  192.168.10.0  0.0.0.0       0             32768 i
* i               192.168.255.2 0      100    0     i
*>i 192.168.200.0 203.0.113.11  0      100    0     64201 i
*>i 192.168.202.0 203.0.113.11  0      100    0     64201 i
*>  192.168.210.0 203.0.113.141 0             0     64202 i
*>  192.168.211.0 203.0.113.141 0             0     64202 i
*>  192.168.212.0 203.0.113.141 0             0     64202 i
*>  192.168.213.0 203.0.113.141 0             0     64202 i
*>  192.168.214.0 203.0.113.141 0             0     64202 i
```

В примере ниже показан вывод команды **show ip bgp** на маршрутизаторе Edge3 после применения политики импорта на обоих маршрутизаторах Edge2 и Edge3.

Пример 261 – Входящие маршруты BGP на маршрутизаторе Edge3 после применения политики импорта

```
admin@Edge3:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.255.3
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network Next  Hop           Metric LocPrf Weight Path
*>  192.168.10.0  0.0.0.0       0             32768  i
* i               192.168.255.2 0      100    0      i
*>i 192.168.200.0 203.0.113.11  0      100    0      64201 i
*>i 192.168.202.0 203.0.113.11  0      100    0      64201 i
*>  192.168.211.0 203.0.113.141 0             0      64202 i
*>  192.168.212.0 203.0.113.141 0             0      64202 i
*>  192.168.214.0 203.0.113.141 0             0      64202 i
```

Фильтрация исходящих маршрутов.

Фильтрация определённых анонсов исходящих маршрутов — это ещё одно основное требование полноценной реализации BGP. В Numa Edge данное требование реализовано посредством использования определённых политик маршрутизации, применяемых к процессу BGP в качестве политики экспорта.

В примере описана настройка исходящих маршрутов таким образом, чтобы AC номер 64200 не предоставляла возможность транзита для AC номер 64201 и AC номер 64202. Таким образом, маршруты узлов eBGP, подключенных к маршрутизатору Edge2 (AC номер 64201), не должны пересылаться узлам eBGP (AC номер 604202), подключенным к маршрутизатору Edge3 и наоборот.

В случае отсутствия фильтрации исходящих маршрутов AC номер 64203 имеет возможность отправлять трафик, предназначенный для AC номер 64202 на маршрутизатор Edge3. В таком случае, этот трафик будет доставляться через сеть AC номер 64200. Есть несколько способов настройки данной политики маршрутизации. В основном применяются настройки, основанные на фильтрации префикса подсети, либо на фильтрации пути AC. В данном примере, как показано на рисунке ниже, вводятся дополнительные ограничения к существующей политики экспорта BGP до, предотвращающие возможность транзита трафика для AC номер 64201 и AC номер 64202 через AC номер 64200.

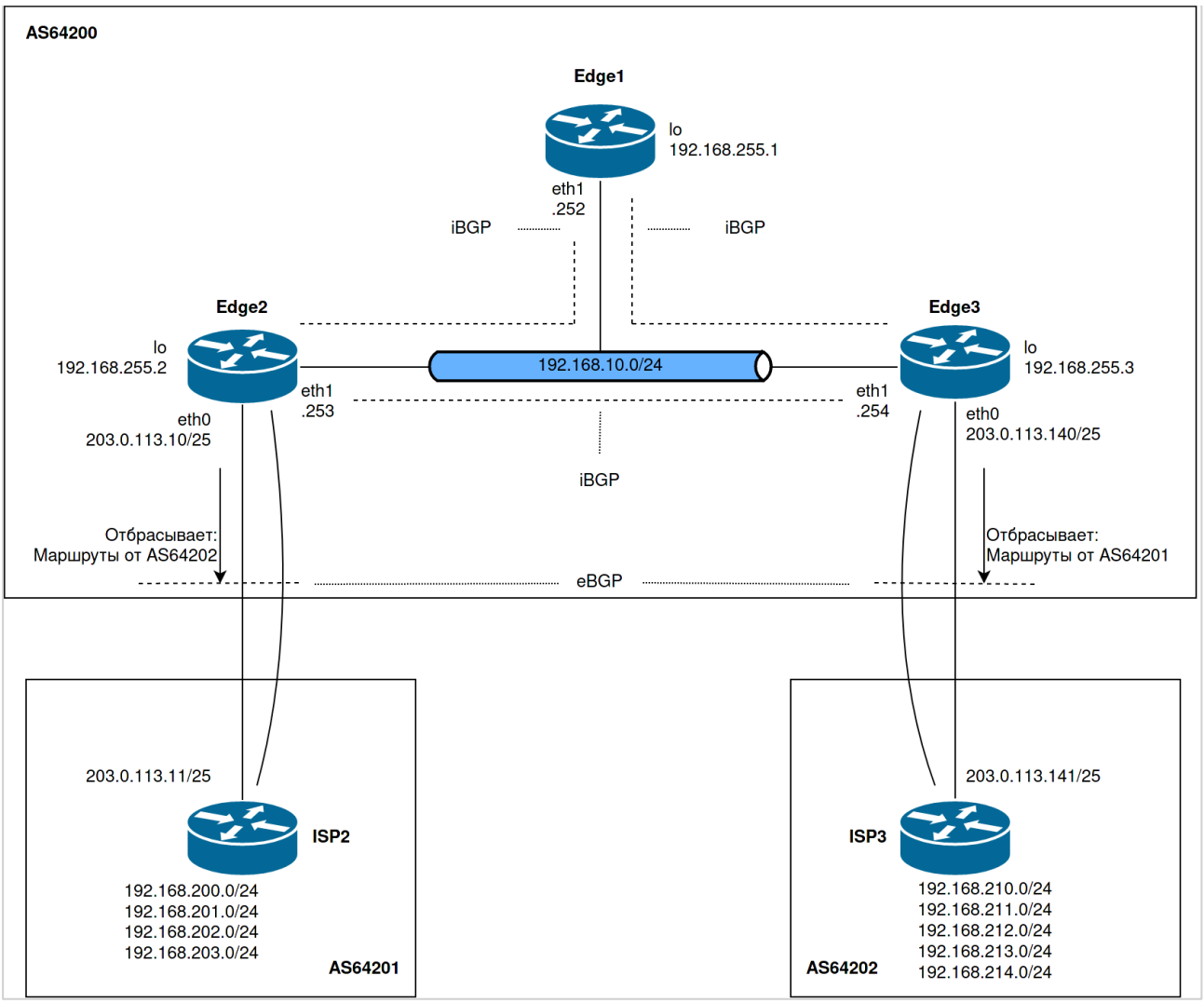


Рисунок 69 – Фильтрация исходящих маршрутов

Для настройки фильтрации исходящих маршрутов необходимо выполнить следующие действия:

Пример 262 – Фильтрация исходящих маршрутов

Настройка маршрутизатора Edge2		
Маршрутизатор	**Действие**	**Команда**

Edge2	Создание списка запрещённых путей АС. Внесение АС номер 64202 в данный список.	`[edit]`
		`admin@Edge2# set policy as-path-list AS64202 rule 1 action permit`
		`[edit]`
		`admin@Edge2# set policy as-path-list AS64202 rule 1 regex 64202`

Edge2	Создание карты маршрутов. Указание правила запрета всех путей, указанных в списке AS64202.	`[edit]`
		`admin@Edge2# set policy route-map eBGP-Export-route rule 10 action deny`
		`[edit]`
		`admin@Edge2# set policy route-map eBGP-Export-route rule 10 match as-path AS64202`

Edge2	Создание правила разрешения всех остальных префиксов подсети в рамках указанной карты маршрутов.	`[edit]` `admin@Edge2# set policy route-map eBGP-Export-route rule 20 action permit`

Edge2	Применение созданной карты маршрутов в качестве политики экспорта для АС с номером 64201.	[edit] admin@Edge2# set protocols bgp 64200 neighbor 203.0.113.11 route-map export eBGP-Export-route
Edge2	Фиксация изменений.	[edit] admin@Edge2# commit
Edge2	Сброс текущей сессии BGP для узла с адресом 203.0.113.11 (для применения созданной политики).	[edit] admin@Edge2# run clear ip bgp 203.0.113.11

Edge2	Вывод настроек текущей конфигурации.	[edit]
		admin@Edge2# show policy as-path-list AS64202
		rule 1 {
		action permit
		regex 64202
		}
		[edit]
		admin@Edge2# show policy route-map eBGP-Export-route
		rule 10 {
		action deny
		match {
		as-path AS64202
		}
		}
		rule 20 {
		action permit
		}

Edge2	Отображение конфигурации BGP для узла eBGP с IP-адресом 203.0.113.11.	[edit]
		admin@Edge2# show protocols bgp 64200 neighbor 203.0.113.11
		remote-as 64201
		route-map {
		export eBGP-Export-route
		import eBGP-Import-route
		}

Настройка маршрутизатора Edge3		
Edge3	Создание списка запрещённых путей АС. Внесение АС номер 64201 в данный список.	[edit] admin@Edge3# set policy as-path-list AS64201 rule 1 action permit [edit] admin@Edge3# set policy as-path-list AS64201 rule 1 regex 64201
Edge3	Создание карты маршрутов. Указание правила запрета всех путей, указанных в списке 64201.	[edit] admin@Edge3# set policy route-map eBGP-Export-route rule 10 action deny [edit] admin@Edge3# set policy route-map eBGP-Export-route rule 10 match as-path AS64201
Edge3	Создание правила разрешения всех остальных префиксов подсети в рамках указанной карты маршрутов.	[edit] admin@Edge3# set policy route-map eBGP-Export-route rule 20 action permit
Edge3	Применение созданной карты маршрутов в качестве политики экспорта для АС с номером 64202.	[edit] admin@Edge3# set protocols bgp 64200 neighbor 203.0.113.141 route-map export eBGP-Export-route

Edge3	Фиксация изменений.	[edit] admin@Edge3# commit
Edge3	Сброс текущей сессии BGP для узла с адресом 203.0.113.141 (для применения созданной политики).	[edit] admin@Edge3# run clear ip bgp 203.0.113.141

Edge3	Вывод настроек текущей конфигурации.	[edit]
		admin@Edge3# show policy as-path-list
		AS64201
		rule 1 {
		action permit
		regex 64201
		}
		[edit]
		admin@Edge3# show policy route-map
		eBGP-Export-route
		rule 10 {
		action deny
		match {
		as-path AS64201
		}
		}
		rule 20 {
		action permit
		}

Edge3	Отображение конфигурации BGP для узла eBGP с IP-адресом 203.0.113.141.	[edit]
		admin@Edge3# show protocols bgp 64200
		neighbor 203.0.113.141
		remote-as 64202
		route-map {
		export eBGP-Export-route
		import eBGP-Import-route
		}

Проверка фильтрации исходящих маршрутов

В примере ниже показана таблица маршрутизации АС номер 64201 до применения политики экспорта.

Пример 263 – Входящие маршруты АС номер 64201 до применения политики экспорта

```
admin@ISP2:~$ show ip bgp
BGP table version is 0, local router ID is 203.0.113.11
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network       Next Hop     Metric LocPrf Weight Path
*> 192.168.10.0  203.0.113.10 0              0      64200  i
*> 192.168.200.0 0.0.0.0      0              32768  i
*> 192.168.201.0 0.0.0.0      0              32768  i
*> 192.168.202.0 0.0.0.0      0              32768  i
*> 192.168.203.0 0.0.0.0      0              32768  i
*> 192.168.211.0 203.0.113.10                0      64200 64202 i
*> 192.168.212.0 203.0.113.10                0      64200 64202 i
*> 192.168.214.0 203.0.113.10                0      64200 64202 i

Displayed 8 out of 8 total prefixes
```

В примере ниже показана таблица маршрутизации АС номер 64201 после применения политики экспорта.

Пример 264 – Входящие маршруты AC номер 64201 после применения политики экспорта

```
admin@ISP2:~$ show ip bgp
BGP table version is 0, local router ID is 203.0.113.11
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop      Metric LocPrf Weight Path
*> 192.168.10.0     203.0.113.10  0              0      64200 i
*> 192.168.200.0    0.0.0.0       0              32768  i
*> 192.168.201.0    0.0.0.0       0              32768  i
*> 192.168.202.0    0.0.0.0       0              32768  i
*> 192.168.203.0    0.0.0.0       0              32768  i

Displayed 5 out of 5 total prefixes
```

Создание конфедерации BGP

Конфедерации позволяют разбивать автономные системы на автономные подсистемы. Подобным образом решается проблема масштабиреумости сетей BGP, связанная с полносвязной конфигурацией соединения всех узлов iBGP в рамках одной AC. В данном примере приведена настройка конфедерации BGP, соответствующая настройке, показанной на рисунке ниже.

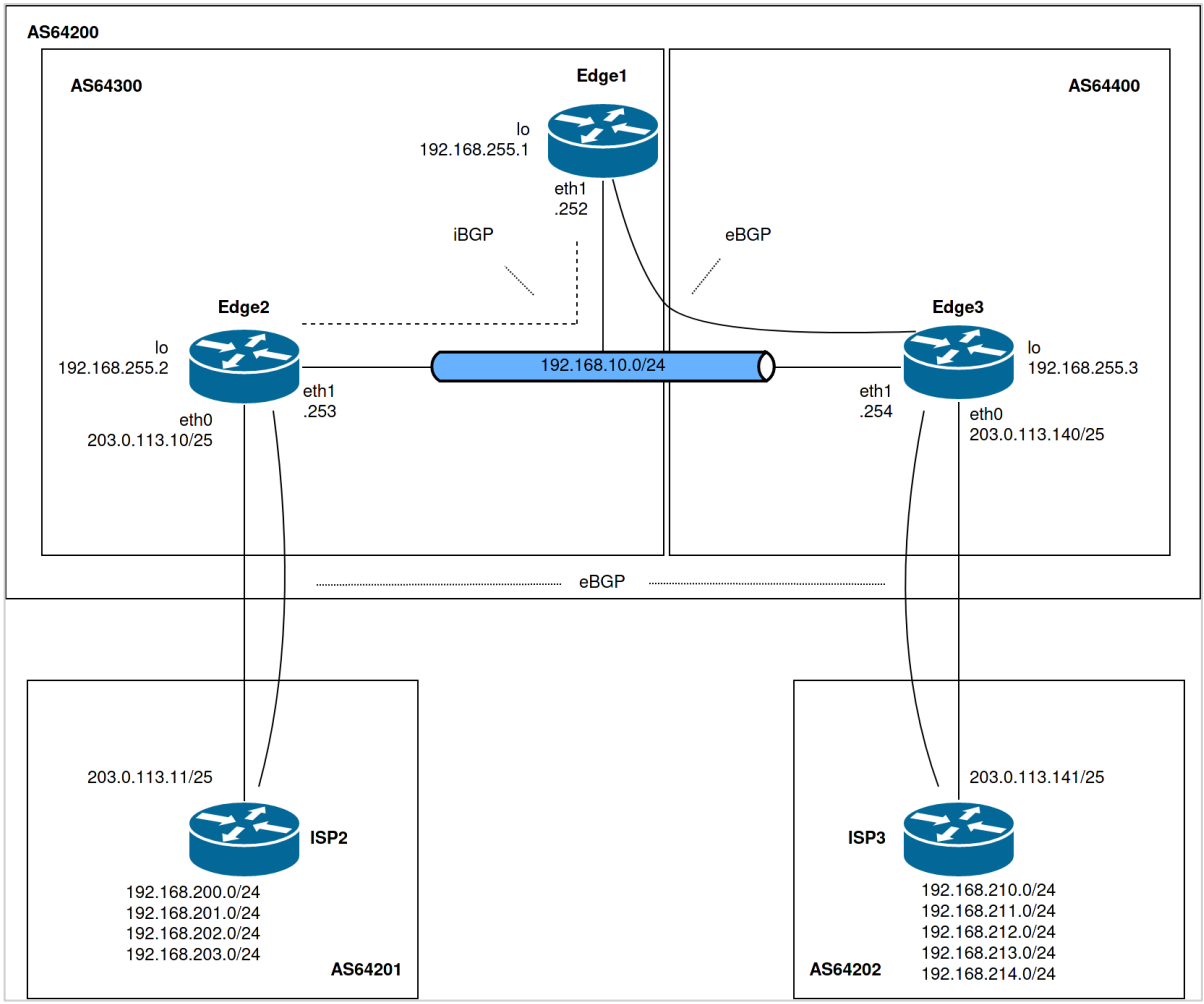


Рисунок 70 – Конфедерация BGP

В данном примере предполагается, что выполнены все настройки, описанные в предыдущих разделах.

Для создания конфедерации BGP необходимо выполнить следующие действия:

Пример 265 – Создание конфедерации BGP.

Настройка маршрутизатора Edge1		
Маршрутизатор	**Действие**	**Команда**
Edge1	Удаление текущей конфигурации BGP.	`[edit]` `admin@Edge1# delete protocols bgp 64200`
Edge1	Создание узла iBGP для маршрутизатора Edge1. Данный маршрутизатор является узлом iBGP, так как находится в той же АС, что и Edge2.	`[edit]` `admin@Edge1# set protocols bgp 64300 neighbor 192.168.255.2 remote-as 64300`
Edge1	Указание IP-адреса маршрутизатора Edge1 в качестве адреса получения обновлений маршрутной информации для маршрутизатора Edge2.	`[edit]` `admin@Edge1# set protocols bgp 64300 neighbor 192.168.255.2 update-source 192.168.255.1`
Edge1	Указание адреса узла eBGP для маршрутизатора Edge1.	`[edit]` `admin@Edge1# set protocols bgp 64300 neighbor 192.168.255.3 remote-as 64400`
Edge1	Указание IP-адреса маршрутизатора Edge1 в качестве адреса получения обновлений маршрутной информации для маршрутизатора Edge3.	`[edit]` `admin@Edge1# set protocols bgp 64300 neighbor 192.168.255.3 update-source 192.168.255.1`
Edge1	Объявление локальной сети для сети BGP.	`[edit]` `admin@Edge1# set protocols bgp 64300 network 192.168.10.0/24`
Edge1	Указание идентификатора АС для конфедерации.	`[edit]` `admin@Edge1# set protocols bgp 64300 parameters confederation identifier 64200`
Edge1	Указание узла для установки соединения с автономной подстанцией.	`[edit]` `admin@Edge1# set protocols bgp 64300 parameters confederation peers 64400`
Edge1	Указание IP-адреса маршрутизатора Edge1 в качестве BGP-ID.	`[edit]` `admin@Edge1# set protocols bgp 64300 parameters router-id 192.168.255.1`
Edge1	Фиксация изменений.	`[edit]` `admin@Edge1# commit`

Edge1	Вывод настроек текущей конфигурации.	`[edit]`
		`admin@Edge1# show protocols bgp`
		`64300 {`
		`  neighbor 192.168.255.2 {`
		`  remote-as 64300`
		`  update-source 192.168.255.1`
		`  }`
		`  neighbor 192.168.255.3 {`
		`  remote-as 64400`
		`  update-source 192.168.255.1`
		`  }`
		`  network 192.168.10.0/24 {`
		`  }`
		`  parameters {`
		`  confederation {`
		`  identifier 64200`
		`  peers 64400`
		`  }`
		`  router-id 192.168.255.1`
		`  }`
		`}`

Настройка маршрутизатора Edge2		
Маршрутизатор	**Действие**	**Команда**
Edge2	Удаление текущей конфигурации BGP.	`[edit]` `admin@Edge2# delete protocols bgp 64200`
Edge2	Указание IP-адреса маршрутизатора Edge2 в качестве адреса следующего транзитного узла для маршрутизатора Edge1.	`[edit]` `admin@Edge2# set protocols bgp 64300 neighbor 192.168.255.1 nexthop-self`
Edge2	Создание узла iBGP для маршрутизатора Edge1. Данный маршрутизатор является узлом iBGP, так как находится в той же АС, что и Edge2.	`[edit]` `admin@Edge2# set protocols bgp 64300 neighbor 192.168.255.1 remote-as 64300`
Edge2	Указание IP-адреса маршрутизатора Edge2 в качестве адреса получения обновлений маршрутной информации для маршрутизатора Edge1.	`[edit]` `admin@Edge2# set protocols bgp 64300 neighbor 192.168.255.1 update-source 192.168.255.2`
Edge2	Указание адреса узла eBGP для маршрутизатора Edge2.	`[edit]` `admin@Edge2# set protocols bgp 64300 neighbor 203.0.113.11 remote-as 64201`
Edge2	Указание карты маршрутов eBGP-Export-route в качестве политики экспорта.	`[edit]` `admin@Edge2# set protocols bgp 64300 neighbor 203.0.113.11 route-map export eBGP-Export-route`
Edge2	Указание карты маршрутов eBGP-Import-route в качестве политики импорта.	`[edit]` `admin@Edge2# set protocols bgp 64300 neighbor 203.0.113.11 route-map import eBGP-Import-route`
Edge2	Объявление локальной сети для сети BGP.	`[edit]` `admin@Edge2# set protocols bgp 64300 network 192.168.10.0/24`
Edge2	Указание идентификатора АС для конфедерации.	`[edit]` `admin@Edge2# set protocols bgp 64300 parameters confederation identifier 64200`
Edge2	Указание узла конфедерации для установки соединения с данной автономной подстанцией.	`[edit]` `admin@Edge2# set protocols bgp 64300 parameters confederation peers 65400`
Edge2	Указание IP-адреса маршрутизатора Edge2 в качестве BGP-ID.	`[edit]` `admin@Edge2# set protocols bgp 64300 parameters router-id 192.168.255.2`
Edge2	Фиксация изменений.	`[edit]` `admin@Edge2# commit`

Edge2	Вывод настроек текущей конфигурации.	`[edit]`
		`admin@Edge2# show protocols bgp 64300 {`
		`  neighbor 192.168.255.1 {`
		`  nexthop-self`
		`  remote-as 64300`
		`  update-source 192.168.255.2`
		`  }`
		`  neighbor 203.0.113.11 {`
		`  remote-as 64201`
		`  route-map {`
		`  export eBGP-Export-route`
		`  import eBGP-Import-route`
		`  }`
		`  }`
		`  network 192.168.10.0/24 {`

Настройка маршрутизатора Edge2		
Маршрутизатор	**Действие**	**Команда**

		}
		parameters {
		confederation {
		identifier 64200
		peers 65400
		}
		router-id 192.168.255.2
		}
		}

Настройка маршрутизатора Edge3		
Маршрутизатор	**Действие**	**Команда**
Edge3	Удаление текущей конфигурации BGP.	[edit] admin@Edge3# delete protocols bgp
Edge3	Указание адреса узла eBGP для маршрутизатора Edge3.	[edit] admin@Edge3# set protocols bgp 64400 neighbor 192.168.255.1 remote-as 64300
Edge3	Указание IP-адреса маршрутизатора Edge3 в качестве адреса получения обновлений маршрутной информации для маршрутизатора Edge1.	[edit] admin@Edge3# set protocols bgp 64400 neighbor 192.168.255.1 update-source 192.168.255.3
Edge3	Указание IP-адреса маршрутизатора Edge3 в качестве адреса следующего транзитного узла для маршрутизатора Edge1.	[edit] admin@Edge3# set protocols bgp 64400 neighbor 192.168.255.1 nexthop-self
Edge3	Указание адреса узла eBGP для маршрутизатора Edge2.	[edit] admin@Edge3# set protocols bgp 64400 neighbor 203.0.113.141 remote-as 64202
Edge3	Указание карты маршрутов eBGP-Export-route в качестве политики экспорта.	[edit] admin@Edge3# set protocols bgp 64400 neighbor 203.0.113.141 route-map export eBGP-Export-route
Edge3	Указание карты маршрутов eBGP-Import-route в качестве политики импорта.	[edit] admin@Edge3# set protocols bgp 64400 neighbor 203.0.113.141 route-map import eBGP-Import-route
Edge3	Объявление локальной сети для сети BGP.	[edit] admin@Edge3# set protocols bgp 64400 network 192.168.10.0/24
Edge3	Указание идентификатора AC для конфедерации.	[edit] admin@Edge3# set protocols bgp 64400 parameters confederation identifier 64200
Edge3	Указание узла конфедерации для установки соединения с данной автономной подстанцией.	[edit] admin@Edge3# set protocols bgp 64400 parameters confederation peers 64300
Edge3	Указание IP-адреса маршрутизатора Edge3 в качестве BGP-ID.	[edit] admin@Edge3# set protocols bgp 64400 parameters router-id 192.168.255.3
Edge3	Фиксация изменений.	[edit] admin@Edge3# commit

Edge3	Вывод настроек текущей конфигурации.	[edit]
		admin@Edge3# show protocols bgp 64400 {
		neighbor 192.168.255.1 {

Настройка маршрутизатора Edge3		
Маршрутизатор	**Действие**	**Команда**

		nexthop-self
		remote-as 64300
		update-source 192.168.255.3
		}
		neighbor 203.0.113.141 {
		remote-as 64202
		route-map {
		export eBGP-Export-route
		import eBGP-Import-route
		}
		}
		network 192.168.10.0/24 {
		}
		parameters {
		confederation {
		identifier 64200
		peers 64300
		}
		router-id 192.168.255.3
		}
		}

Проверка конфигурации BGP

В примере ниже показан вывод команды **show ip bgp summary** на маршрутизаторе Edge1.

Пример 266 – Проверка конфедерации BGP на маршрутизаторе Edge1: вывод кратких сведений о состоянии соединения BGP

```
admin@Edge1:~$ show ip bgp summary
BGP router identifier 192.168.255.1, local AS number 64300
RIB entries 11, using 1232 bytes of memory
Peers 2, using 18 KiB of memory

Neighbor        V    AS MsgRcvd MsgSent OutQ Up/Down  State         PfxRcd
192.168.255.2   4 64300      24      20    0 00:09:39 Established        3
192.168.255.3   4 64400      20      21    0 00:00:19 Established        4

Total number of neighbors 2

Total num. Established sessions 2
Total num. of routes received     7
```

В примере ниже показан вывод команды **show ip bgp** на маршрутизаторе Edge1.

Пример 267 – Проверка конфедерации на маршрутизаторе Edge1: вывод сведений о составе таблицы маршрутизации BGP

```
admin@Edge1:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.255.1
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network Next  Hop           Metric LocPrf Weight Path
*   192.168.10.0  192.168.255.3 0      100    0      (64400) i
* i               192.168.255.2 0      100    0      i
*>                0.0.0.0       0              32768  i
*>i 192.168.200.0 192.168.255.2 0      100    0      64201 i
*>i 192.168.202.0 192.168.255.2 0      100    0      64201 i
*>  192.168.211.0 192.168.255.3 0      100    0      (64400) 64202 i
*>  192.168.212.0 192.168.255.3 0      100    0      (64400) 64202 i
*>  192.168.214.0 192.168.255.3 0      100    0      (64400) 64202 i

Displayed 6 out of 8 total prefixes
```

Следует отметить, что все маршруты, полученные от маршрутизатора Edge3 (Next Hop 192.168.255.3) содержат номер автономной подсистемы в атрибуте AS_PATH. Номера всех автономных подсистем, состоящих в данной конфедерации заключены в скобки (). Номера автономных подсистем не передаются за пределы автономной системы, в которой состоит данная конфедерация (AC номер 64200).

В примере ниже показан вывод команды **show ip bgp summary** на маршрутизаторе Edge2.

Пример 268 – Проверка конфедерации BGP на маршрутизаторе Edge2: вывод кратких сведений о состоянии соединения BGP

```
admin@Edge2:~$ show ip bgp summary
BGP router identifier 192.168.255.2, local AS number 64300
RIB entries 11, using 1232 bytes of memory
Peers 2, using 18 KiB of memory

Neighbor        V    AS MsgRcvd MsgSent OutQ Up/Down  State         PfxRcd
192.168.255.1   4 64300       5       6    0 00:00:53 Established        4
203.0.113.11    4 64201       5       6    0 00:01:49 Established        2

Total number of neighbors 2

Total num. Established sessions 2
Total num. of routes received     6
```

В примере ниже показан вывод команды **show ip bgp** на маршрутизаторе Edge2.

Пример 269 – Проверка конфедерации на маршрутизаторе Edge2: вывод сведений о составе таблицы маршрутизации BGP

```
admin@Edge2:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.255.2
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network Next  Hop           Metric LocPrf Weight Path
* i 192.168.10.0  192.168.255.1 0      100    0      i
*>                0.0.0.0       0              32768  i
*>  192.168.200.0 203.0.113.11  0              0      64201 i
*>  192.168.202.0 203.0.113.11  0              0      64201 i
*>i 192.168.211.0 192.168.255.3 0      100    0      (64400) 64202 i
*>i 192.168.212.0 192.168.255.3 0      100    0      (64400) 64202 i
*>i 192.168.214.0 192.168.255.3 0      100    0      (64400) 64202 i

Displayed 6 out of 7 total prefixes
```

В примере ниже показан вывод команды **show ip bgp summary** на маршрутизаторе Edge3.

Пример 270 – Проверка конфедерации BGP на маршрутизаторе Edge3: вывод кратких сведений о состоянии соединения BGP

```
admin@Edge3:~$ show ip bgp summary
BGP router identifier 192.168.255.3, local AS number 64400
RIB entries 11, using 1232 bytes of memory
Peers 2, using 18 KiB of memory

Neighbor        V    AS MsgRcvd MsgSent OutQ Up/Down  State         PfxRcd
192.168.255.1   4 64300       5       6    0 00:00:15 Established        3
203.0.113.141   4 64202       5       6    0 00:01:05 Established        3

Total number of neighbors 2

Total num. Established sessions 2
Total num. of routes received     6
```

В примере ниже показан вывод команды **show ip bgp** на маршрутизаторе Edge3.

Пример 271 – Проверка конфедерации на маршрутизаторе Edge3: вывод сведений о составе таблицы маршрутизации BGP

```
admin@Edge3:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.255.3
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network       Next Hop      Metric LocPrf Weight Path
   192.168.10.0  192.168.255.1 0      100    0      (64300) i
*>               0.0.0.0       0                    32768 i
*> 192.168.200.0 192.168.255.2 0      100    0      (64300) 64201 i
*> 192.168.202.0 192.168.255.2 0      100    0      (64300) 64201 i
*> 192.168.211.0 203.0.113.141 0             0      64202 i
*> 192.168.212.0 203.0.113.141 0             0      64202 i
*> 192.168.214.0 203.0.113.141 0             0      64202 i

Displayed 6 out of 7 total prefixes
```

Отражатели маршрутов

Как и конфедерации, отражатели маршрутов также применяются для решения проблемы масштабируемости BGP. Конфигурация отражателя маршрутов подразумеваем наличие в сети, по крайней мере, одного сервера отражателя маршрутов и одного или нескольких клиентов отражателя маршрутов. В примере, показанном на рисунке представленном ниже, маршрутизатор Edge1 является сервером отражателя маршрутов, а маршрутизаторы Edge2 и Edge3 – клиентами отражателя маршрутов.

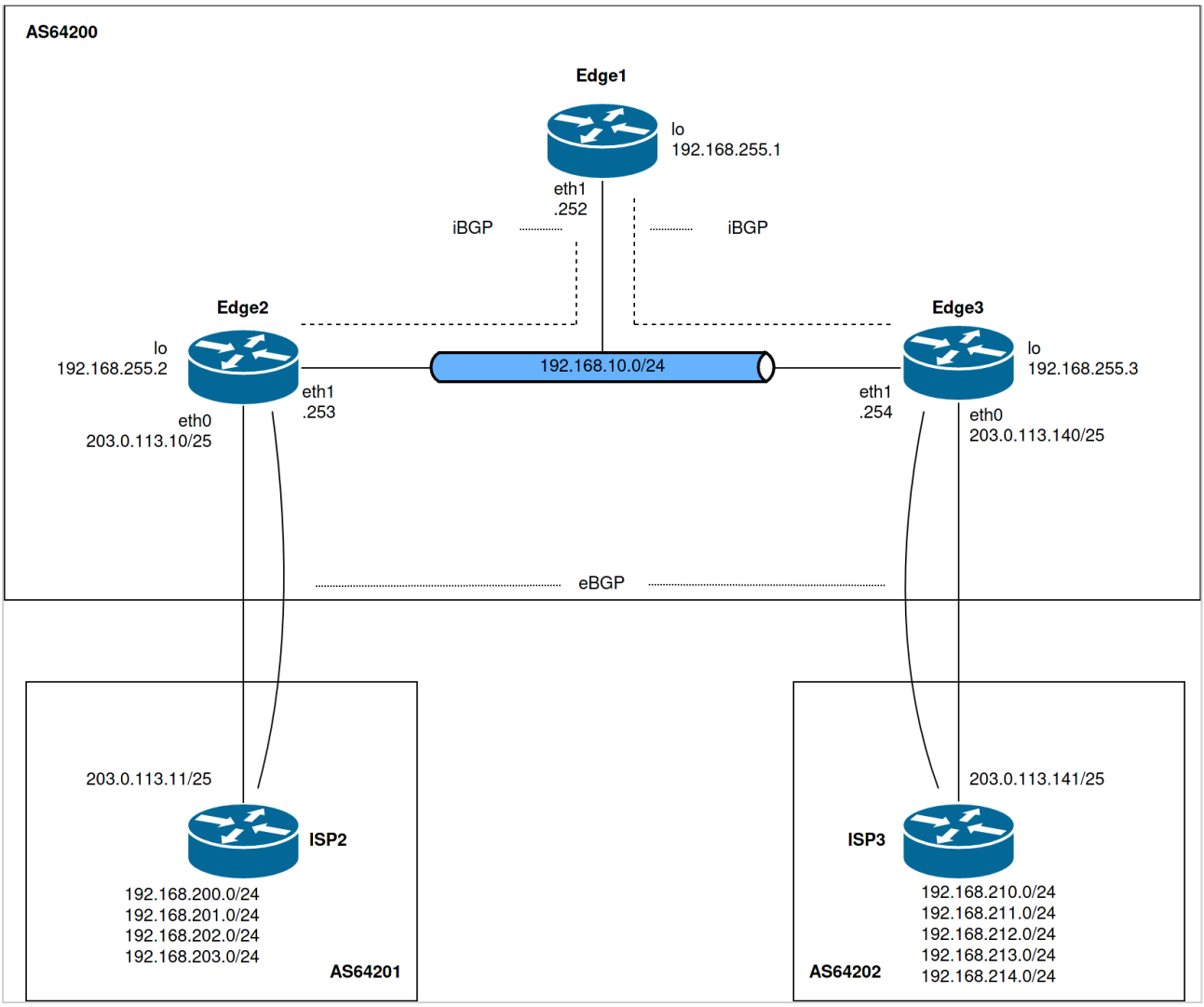


Рисунок 71 – Отражатель маршрутов BGP

В данном примере предполагается, что выполнены все настройки, описанные в предыдущих разделах. Если настройка производится с использованием базовой конфигурации, то следует пропустить первое действие (удаление предыдущей конфигурации BGP).

Для создания отражателя маршрутов BGP необходимо выполнить следующие действия:

Пример 272 – Создание отражателя маршрутов BGP

Настройка маршрутизатора Edge1		
Маршрутизатор	**Действие**	**Команда**
Edge1	Удаление текущей конфигурации BGP.	`[edit]` `admin@Edge1# delete protocols bgp`
Edge1	Создание узла iBGP для маршрутизатора Edge2. Данный маршрутизатор является узлом iBGP, так как находится в той же АС, что и Edge1.	`[edit]` `admin@Edge1# set protocols bgp 64200 neighbor 192.168.255.2 remote-as 64200`
Edge1	Определение маршрутизатора Edge2 в качестве клиента отражателя маршрутов.	`[edit]` `admin@Edge1# set protocols bgp`

Настройка маршрутизатора Edge1		
Маршрутизатор	**Действие**	**Команда**
		`64200 neighbor 192.168.255.2 route-reflector-client`
Edge1	Указание IP-адреса маршрутизатора Edge1 в качестве адреса получения обновлений маршрутной информации для маршрутизатора Edge2.	`[edit]` `admin@Edge1# set protocols bgp 64200 neighbor 192.168.255.2 update-source 192.168.255.1`
Edge1	Создание узла iBGP для маршрутизатора Edge3. Данный маршрутизатор является узлом iBGP, так как находится в той же АС, что и Edge1.	`[edit]` `admin@Edge1# set protocols bgp 64200 neighbor 192.168.255.3 remote-as 64200`
Edge1	Определение маршрутизатора Edge3 в качестве клиента отражателя маршрутов.	`[edit]` `admin@Edge1# set protocols bgp 64200 neighbor 192.168.255.3 route-reflector-client`
Edge1	Указание IP-адреса маршрутизатора Edge1 в качестве адреса получения обновлений маршрутной информации для маршрутизатора Edge3.	`[edit]` `admin@Edge1# set protocols bgp 64200 neighbor 192.168.255.3 update-source 192.168.255.1`
Edge1	Объявление локальной сети для сети BGP.	`[edit]` `admin@Edge1# set protocols bgp 64200 network 192.168.10.0/24`
Edge1	Указание IP-адреса маршрутизатора Edge1 в качестве BGP-ID.	`[edit]` `admin@Edge1# set protocols bgp 64200 parameters router-id 192.168.255.1`
Edge1	Фиксация изменений.	`[edit]` `admin@Edge1# commit`

Edge1	Вывод настроек текущей конфигурации.	`[edit]`
		`admin@Edge1# show protocols bgp`
		`64200 {`
		`  neighbor  192.168.255.2 {`
		`  remote-as 64200`
		`  route-reflector-client`
		`  update-source 192.168.255.1`
		`  }`
		`  neighbor 192.168.255.3 {`
		`  remote-as 64200`
		`  route-reflector-client`
		`  update-source 192.168.255.1`
		`  }`
		`  network 192.168.10.0/24 {`
		`  }`
		`  parameters {`
		`  router-id 192.168.255.1`
		`  }`
		`}`

Настройка маршрутизатора Edge2		
Маршрутизатор	**Действие**	**Команда**
Edge2	Удаление текущей конфигурации BGP.	`[edit]` `admin@Edge2# delete protocols bgp`
Edge2	Указание IP-адреса маршрутизатора Edge2 в качестве адреса следующего транзитного узла для маршрутизатора Edge1.	`[edit]` `admin@Edge2# set protocols bgp 64200 neighbor 192.168.255.1 nexthop-self`
Edge2	Создание узла iBGP для маршрутизатора	`[edit]`

Настройка маршрутизатора Edge2		
Маршрутизатор	**Действие**	**Команда**
	Edge1. Данный маршрутизатор является узлом iBGP, так как находится в той же AC, что и Edge2.	`admin@Edge2# set protocols bgp 64200 neighbor 192.168.255.1 remote-as 64200`
Edge2	Указание IP-адреса маршрутизатора Edge2 в качестве адреса получения обновлений маршрутной информации для маршрутизатора Edge1.	`[edit]` `admin@Edge2# set protocols bgp 64200 neighbor 192.168.255.1 update-source 192.168.255.2`
Edge2	Указание адреса узла eBGP для маршрутизатора Edge2.	`[edit]` `admin@Edge2# set protocols bgp 64200 neighbor 203.0.113.11 remote-as 64201`
Edge2	Указание карты маршрутов eBGP-Export-route в качестве политики экспорта.	`[edit]` `admin@Edge2# set protocols bgp 64200 neighbor 203.0.113.11 route-map export eBGP-Export-route`
Edge2	Указание карты маршрутов eBGP-Import-route в качестве политики импорта.	`[edit]` `admin@Edge2# set protocols bgp 64200 neighbor 203.0.113.11 route-map import eBGP-Import-route`
Edge2	Объявление локальной сети для сети BGP.	`[edit]` `admin@Edge2# set protocols bgp 64200 network 192.168.10.0/24`
Edge2	Указание IP-адреса маршрутизатора Edge2 в качестве BGP-ID.	`[edit]` `admin@Edge2# set protocols bgp 64200 parameters router-id 192.168.255.2`
Edge2	Фиксация изменений.	`[edit]` `admin@Edge2# commit`

Edge2	Вывод настроек текущей конфигурации.	`[edit]`
		`admin@Edge2# show protocols bgp`
		`64200 {`
		`  neighbor 192.168.255.1 {`
		`  nexthop-self`
		`  remote-as 64200`
		`  update-source 192.168.255.2`
		`  }`
		`  neighbor 203.0.113.11 {`
		`  remote-as 64201`
		`  route-map {`
		`  export eBGP-Export-route`
		`  import eBGP-Import-route`
		`  }`
		`  }`
		`  network 192.168.10.0/24 {`
		`  }`
		`  parameters {`
		`  router-id 192.168.255.2`
		`  }`
		`}`

Настройка маршрутизатора Edge3		
Маршрутизатор	**Действие**	**Команда**
Edge3	Удаление текущей конфигурации BGP.	`[edit]` `admin@Edge3# delete protocols bgp`
Edge3	Указание IP-адреса маршрутизатора Edge3 в качестве адреса следующего транзитного	`[edit]` `admin@Edge3# set protocols bgp 64200 neighbor 192.168.255.1`

Настройка маршрутизатора Edge3		
Маршрутизатор	**Действие**	**Команда**
	узла для маршрутизатора Edge1.	`nexthop-self`
Edge3	Создание узла iBGP для маршрутизатора Edge1. Данный маршрутизатор является узлом iBGP, так как находится в той же AC, что и Edge3.	`[edit]` `admin@Edge3# set protocols bgp 64200 neighbor 192.168.255.1 remote-as 64200`
Edge3	Указание IP-адреса маршрутизатора Edge3 в качестве адреса получения обновлений маршрутной информации для маршрутизатора Edge1.	`[edit]` `admin@Edge3# set protocols bgp 64200 neighbor 192.168.255.1 update-source 192.168.255.3`
Edge3	Указание адреса узла eBGP для маршрутизатора Edge3.	`[edit]` `admin@Edge3# set protocols bgp 64200 neighbor 203.0.113.141 remote-as 64202`
Edge3	Указание карты маршрутов eBGP-Export-route в качестве политики экспорта.	`[edit]` `admin@Edge3# set protocols bgp 64200 neighbor 203.0.113.141 route-map export eBGP-Export-route`
Edge3	Указание карты маршрутов eBGP-Import-route в качестве политики импорта.	`[edit]` `admin@Edge3# set protocols bgp 64200 neighbor 203.0.113.141 route-map import eBGP-Import-route`
Edge3	Объявление локальной сети для сети BGP.	`[edit]` `admin@Edge3# set protocols bgp 64200 network 192.168.10.0/24`
Edge3	Указание IP-адреса маршрутизатора Edge3 в качестве BGP-ID.	`[edit]` `admin@Edge3# set protocols bgp 64200 parameters router-id 192.168.255.3`
Edge3	Фиксация изменений.	`[edit]` `admin@Edge3# commit`

Edge3	Вывод настроек текущей конфигурации.	`[edit]`
		`admin@Edge3# show protocols bgp`
		`64200 {`
		`  neighbor 192.168.255.1 {`
		`  nexthop-self`
		`  remote-as 64200`
		`  update-source 192.168.255.3`
		`  }`
		`  neighbor 203.0.113.141 {`
		`  remote-as 64202`
		`  route-map {`
		`  export eBGP-Export-route`
		`  import eBGP-Import-route`
		`  }`
		`  }`
		`  network 192.168.10.0/24 {`
		`  }`
		`  parameters {`
		`  router-id 192.168.255.3`
		`  }`
		`}`

Проверка отражателя маршрутов

В примере ниже показан вывод команды **show ip bgp summary** на маршрутизаторе Edge1.

Пример 273 – Проверка отражателя маршрутов на маршрутизаторе Edge1: вывод кратких сведений о состоянии соединения BGP

```
admin@Edge1:~$ show ip bgp summary
BGP router identifier 192.168.255.1, local AS number 64200
RIB entries 11, using 1232 bytes of memory
Peers 2, using 18 KiB of memory

Neighbor        V    AS MsgRcvd MsgSent OutQ Up/Down  State         PfxRcd
192.168.255.2   4 64200      12      13    0 00:00:44 Established        3
192.168.255.3   4 64200      13      14    0 00:00:03 Established        4

Total number of neighbors 2

Total num. Established sessions 2
Total num. of routes received     7
```

В примере ниже показан вывод команды **show ip bgp** на маршрутизаторе Edge1.

Пример 274 – Проверка отражателя маршрутов Edge1: вывод сведений о составе таблицы маршрутизации BGP

```
admin@Edge1:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.255.1
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network       Next Hop      Metric LocPrf Weight Path
* i 192.168.10.0  192.168.255.2 0      100    0      i
* i               192.168.255.3 0      100    0      i
*>                0.0.0.0       0             32768  i
*>i 192.168.200.0 192.168.255.2 0      100    0      64201 i
*>i 192.168.202.0 192.168.255.2 0      100    0      64201 i
*>i 192.168.211.0 192.168.255.3 0      100    0      64202 i
*>i 192.168.212.0 192.168.255.3 0      100    0      64202 i
*>i 192.168.214.0 192.168.255.3 0      100    0      64202 i

Displayed 6 out of 8 total prefixes
```

В примере ниже показан вывод команды **show ip bgp summary** на маршрутизаторе Edge2.

Пример 275 – Проверка отражателя маршрутов на маршрутизаторе Edge2: вывод кратких сведений о состоянии соединения BGP

```
admin@Edge2:~$ show ip bgp summary
BGP router identifier 192.168.255.2, local AS number 64200
RIB entries 11, using 1232 bytes of memory
Peers 2, using 18 KiB of memory

Neighbor        V    AS MsgRcvd MsgSent OutQ Up/Down  State         PfxRcd
192.168.255.1   4 64200       5      13    0 00:01:28 Established        4
203.0.113.11    4 64201       4       7    0 00:01:57 Established        2

Total number of neighbors 2

Total num. Established sessions 2
Total num. of routes received     6
```

В примере ниже показан вывод команды **show ip bgp** на маршрутизаторе Edge2.

Пример 276 – Проверка отражателя маршрутов Edge2: вывод сведений о составе таблицы маршрутизации BGP

```
admin@Edge2:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.255.2
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network       Next Hop      Metric LocPrf Weight Path
* i 192.168.10.0  192.168.255.1 0      100    0      i
*>                0.0.0.0       0              32768  i
*>  192.168.200.0 203.0.113.11  0              0      64201 i
*>  192.168.202.0 203.0.113.11  0              0      64201 i
*>i 192.168.211.0 192.168.255.3 0      100    0      64202 i
*>i 192.168.212.0 192.168.255.3 0      100    0      64202 i
*>i 192.168.214.0 192.168.255.3 0      100    0      64202 i
```

В примере ниже показан вывод команды **show ip bgp summary** на маршрутизаторе Edge3.

Пример 277 – Проверка отражателя маршрутов на маршрутизаторе Edge3: вывод кратких сведений о состоянии соединения BGP

```
admin@Edge3:~$ show ip bgp summary
BGP router identifier 192.168.255.3, local AS number 64200
RIB entries 11, using 1232 bytes of memory
Peers 2, using 18 KiB of memory

Neighbor        V    AS MsgRcvd MsgSent OutQ Up/Down  State         PfxRcd
192.168.255.1   4 64200       5      11    0 00:01:19 Established        3
203.0.113.141   4 64202       5       6    0 00:01:39 Established        3

Total number of neighbors 2

Total num. Established sessions 2
Total num. of routes received     6
```

В примере ниже показан вывод команды **show ip bgp** на маршрутизаторе Edge3.

Пример 278 – Проверка отражателя маршрутов Edge3: вывод сведений о составе таблицы маршрутизации BGP

```
admin@Edge3:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.255.3
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network       Next Hop      Metric LocPrf Weight Path
* i 192.168.10.0  192.168.255.1 0      100    0      i
*>                0.0.0.0       0              32768  i
*>i 192.168.200.0 192.168.255.2 0      100    0      64201 i
*>i 192.168.202.0 192.168.255.2 0      100    0      64201 i
*>  192.168.211.0 203.0.113.141 0              0      64202 i
*>  192.168.212.0 203.0.113.141 0              0      64202 i
*>  192.168.214.0 203.0.113.141 0              0      64202 i

Displayed 6 out of 7 total prefixes
```

28.2 Группы узлов

Конфигурационные команды	
protocols bgp <номер_АС> peer-group <имя_группы>	Указание группы узлов BGP.
protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast	Определение конфигурации однонаправленных IPv6-маршрутов BGP для пиринговой сессии.
protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast allowas-in	Разрешение на получение объявления, содержащего атрибут AS_PATH локальному маршрутизатору.
protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast attribute-unchanged	Разрешение локальному маршрутизатору передачи обновлений группе узлов с неизменными атрибутами.
protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast capability dynamic	Объявление поддержки динамического обновления, получаемого от группы узлов.
protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast capability orf	Объявление поддержки Outbound Route Filtering (ORF), получаемого от группы узлов.
protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast default-originate	Разрешение пересылки маршрута по умолчанию группе узлов.
protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast disable-send-community	Запрещение отправки расширенных атрибутов к указанной группе узлов.
protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast distribute-list export <список_доступа>	Применение списка доступа для фильтрации исходящих обновлений маршрутизации к группе узлов.
protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast distribute-list import <список_доступа>	Применение списка доступа для фильтрации входящих обновлений маршрутизации от группы узлов.
protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast filter-list export <имя_списка_путей>	Применение список пути AS к маршрутным обновлениям до указанной группы узлов.
protocols bgp <номер_АС> peer-group <group-name> address-family ipv6-unicast filter-list import <имя_списка_путей>	Применение список пути AS к маршрутным обновлениям от указанной группы узлов.
protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast maximum-prefix <число_префиксов>	Установка максимального числа префиксов, принимаемых группой узлов перед тем как она будет переведена в нерабочее состояние.
protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast nexthop-local unchanged	Указание IPv6-адреса, не изменяемого при анонсировании префикса узлом.
protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast nexthop-self	Установка локального маршрутизатора как следующего транзитного участка для группы узлов.
protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast prefix-list export <имя_префикс-листа>	Применение префиксного списка для фильтрации обновлений к группе узлов.
protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast prefix-list import <имя_префикс-листа>	Применение префиксного списка для фильтрации обновлений от группы узлов.
protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast remove-private-as	Предписание локальному маршрутизатору на исключение частных АС от обновлений.
protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast route-map export <имя_карты_маршрутов>	Применение карты маршрута для фильтрации обновлений к группе узлов.
protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast route-map import <имя_карты_маршрутов>	Применение карты маршрута для фильтрации обновлений от группы узлов.
protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast soft-reconfiguration inbound	Предписание локальному маршрутизатору на сохранение полученных маршрутных обновлений.

protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast unsuppress-map <имя_карты_маршрутов>	Предписание локальному маршрутизатору выборочно распространять маршруты на основе маршрутной карты.
protocols bgp <номер_АС> peer-group <имя_группы> attribute-unchanged	Разрешение локальному маршрутизатору передачи обновлений группе узлов с неизменными атрибутами.
protocols bgp <номер_АС> peer-group <имя_группы> allowas-in	Разрешение на получение объявления, содержащего путь АС локального маршрутизатора.
protocols bgp <номер_АС> peer-group <имя_группы> capability orf	Разрешение локальному маршрутизатору передачи обновлений группе узлов с неизменными атрибутами.
protocols bgp <номер_АС> peer-group <имя_группы> remote-as <номер_удаленной_АС>	Разрешение локальному маршрутизатору передачи обновлений группе узлов с неизменными атрибутами
protocols bgp <номер_АС> peer-group <имя_группы> capability dynamic	Объявление поддержки динамического обновления, получаемого от группы узлов.
protocols bgp <номер_АС> peer-group <имя_группы> capability orf	Объявление поддержки Outbound Route Filtering (ORF), получаемого от группы узлов.
protocols bgp <номер_АС> peer-group <имя_группы> default-originate	Разрешение пересылки маршрута по умолчанию группе узлов.
protocols bgp <номер_АС> peer-group <имя_группы> description <описание>	Краткое описание группы узлов.
protocols bgp <номер_АС> peer-group <имя_группы> disable-capability-negotiation	Отключение согласования возможностей BGP.
protocols bgp <номер_АС> peer-group <имя_группы> disable-connected-check	Отключение проверки прямого подключения для транзитного узла.
protocols bgp <номер_АС> peer-group <имя_группы> disable-send-community	Запрещение отправки расширенных атрибутов к указанной группе узлов.
protocols bgp <номер_АС> peer-group <имя_группы> distribute-list export <список_доступа>	Применение списка допуска, для фильтрации исходящих маршрутных обновлений группы узлов.
protocols bgp <номер_АС> peer-group <имя_группы> distribute-list import <список_доступа>	Применение списка допуска, для фильтрации входящих маршрутных обновлений группы узлов.
protocols bgp <номер_АС> peer-group <имя_группы> ebgp-multihop <количество_переходов>	Предоставление участия в динамической маршрутизации узлам, не соединенным напрямую.
protocols bgp <номер_АС> peer-group <имя_группы> filter-list export <имя_списка_путей>	Применение списка пути AS к маршрутным обновлениям до указанной группы узлов.
protocols bgp <номер_АС> peer-group <имя_группы> filter-list import <имя_списка_путей>	Применение списка пути AS к маршрутным обновлениям до указанной группы узлов.
protocols bgp <номер_АС> peer-group <имя_группы> local-as <номер_локальной_АС>	Указание номера локальной АС для равноправных узлов.
protocols bgp <номер_АС> peer-group <имя_группы> maximum-prefix <число_префиксов>	Установка максимального числа префиксов, принимаемых группой узлов перед тем как она будет переведена в нерабочее состояние.
protocols bgp <номер_АС> peer-group <group-name> nexthop-self	Установка локального маршрутизатора как следующего транзитного участка для группы узлов.
protocols bgp <номер_АС> peer-group <имя_группы> override-capability	Разрешение на пиринговую сессию с группой узлов, которая не поддерживает согласование возможностей.
protocols bgp <номер_АС> peer-group <имя_группы> passive	Предписание маршрутизатору не инициировать соединение указанной группой узлов.
protocols bgp <номер_АС> peer-group <имя_группы> password <пароль>	Указание хешированного в MD5 пароля.
protocols bgp <номер_АС> peer-group <имя_группы> prefix-list export <имя_префикс-листа>	Применение префиксного списка для фильтрации обновлений к группе узлов.
protocols bgp <номер_АС> peer-group <имя_группы> prefix-list import <имя_префикс-листа>	Применение префиксного списка для фильтрации обновлений от группы узлов.

protocols bgp <номер_AC> peer-group <имя_группы> remove-private-as	Предписание локальному маршрутизатору на исключение частных AC от обновлений.
protocols bgp <номер_AC> peer-group <имя_группы> shutdown	Административное прекращение работы группы узлов.
protocols bgp <номер_AC> peer-group <имя_группы> soft-reconfiguration inbound	Предписание локальному маршрутизатору на сохранение полученных маршрутных обновлений.
protocols bgp <номер_AC> peer-group <имя_группы> ttl-security hops <число_переходов>	Установка TTL для транзитных участков для указанной группы узлов
protocols bgp <номер_AC> peer-group <имя_группы> unsuppress-map <имя_карты_маршрутов>	Предписание локальному маршрутизатору выборочно распространять маршруты на основе маршрутной карты.
protocols bgp <номер_AC> peer-group <имя_группы> update-source	Определение исходного IP-адреса или интерфейса маршрутных обновлений.
protocols bgp <номер_AC> peer-group <имя_группы> weight <вес>	Определение веса по умолчанию для маршрутов от группы узлов.
Операционные команды	
clear ip bgp peer-group <group-name>	Сброс пиринговой сессии для всех членов группы узлов.
clear ip bgp peer-group <group-name> ipv4 unicast	Сброс IPv4-сессии для всех членов группы узлов.

28.2.1 protocols bgp <номер_AC> peer-group <имя_группы>

Указание группы узлов BGP.

Синтаксис

```
set protocols bgp <номер_AC> peer-group  <имя_группы>
delete protocols bgp <номер_AC> peer-group <имя_группы>
show protocols bgp <номер_AC> peer-group <имя_группы>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы{
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Многоузловой. Название группы узлов.

Значение по умолчанию

Отсутствует.

Указания по использованию

При необходимости настройки нескольких узлов BGP с одинаковыми параметрами возможно использование групп узлов. Настройка групп узлов происходит таким же образом, как настройка отдельных

узлов. При применения какой-либо настройки к группе узлов, данная настройка применяется ко всем узлам, состоящим в данной группе.

Форма **set** этой команды используется для указания группы узлов BGP.

Форма **delete** этой команды используется для удаления группы узлов BGP.

Форма **show** этой команды используется для просмотра настройки конфигурации группы узлов BGP.

28.2.2 protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast

Определение конфигурации однонаправленных IPv6-маршрутов BGP для пиринговой сессии.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast

delete protocols bgp <номер_AC>peer-group <имя_группы> address-family ipv6-unicast

show protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-groupимя_группы{
         address-family {
            ipv6-unicast {
            }
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

имя_группы

Многоузловой. Название группы узлов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Использование этой команды определяет конфигурацию однонаправленных IPv6-маршрутов BGP для пиринговой сессии

Форма **set** этой команды используется для определения конфигурации группы узлов.

Форма **delete** этой команды используется для удаления конфигурации группы узлов.

Форма **show** этой команды используется для просмотра настройки конфигурации группы узлов.

28.2.3 protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast allowas-in

Разрешение на получение объявления, содержащего атрибут AS_PATH локальному маршрутизатору.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast allowas-in [number <количество>]

delete protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast allowas-in [number]

show protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        peer-group имя_группы
            address-family {
                ipv6-unicast {
                    allowas-in {
                        number количество
                    }
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

number количество

Количество попыток на получение объявления, атрибута AS_PATH локальному маршрутизатору. Диапазон составляет от 1 до 10 попыток. По умолчанию установлено 3 попытки.

Значение по умолчанию

Получение объявления атрибута AS_PATH запрещено.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для разрешения локальному маршрутизатору принимать объявления атрибута AS_PATH.

Форма **delete** этой команды используется для запрещения локальному маршрутизатору принимать объявления атрибута AS_PATH.

Форма **show** этой команды используется для просмотра настройки конфигурации.

28.2.4 protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast attribute-unchanged

Разрешение локальному маршрутизатору передачи обновлений группе узлов с неизменными атрибутами.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast attribute-unchanged [as-path|med|next-hop]

delete protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast attribute-unchanged [as-path|med|next-hop]

show protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast attribute-unchanged
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        peer-group имя_группы
            address-family {
                ipv6-unicast {
                    attribute-unchanged {
                        as-path
                        med
                        next-hop
                    }
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

as-path

Распространение обновлений маршрутов с неизменным атрибутом AS_PATH.

med

Распространение обновлений маршрутов с неизменным атрибутом Multi Exit Discriminator.

next-hop

Распространение обновлений маршрутов с неизменным атрибутом next-hop.

Значение по умолчанию

Запрещено.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для разрешения передачи локальным маршрутизатором обновлений маршрутов, без изменения атрибутов BGP: AS_PATH, MED и next-hop.

Форма **delete** этой команды используется для восстановления нормальной модификации атрибутов BGP.

Форма **show** этой команды используется для просмотра настройки конфигурации.

28.2.5 protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast capability dynamic

Объявление поддержки динамического обновления, получаемого от группы узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast capability dynamic

delete protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast capability dynamic

show protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        peer-group имя_группы
          address-family {
              ipv6-unicast {
                 capability {
                    dynamic
                 }
              }
           }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

Значение по умолчанию

Пиринговая сессия функционирует с минимальными возможностями.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для объявления поддержки динамического обновления, получаемого от группы узлов.

Форма **delete** этой команды используется для отказа возможности динамического обновления.

Форма **show** этой команды используется для просмотра настройки конфигурации.

28.2.6 protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast capability orf

Объявление поддержки Outbound Route Filtering (ORF), получаемого от группы узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast capability orf [prefix-list [receive | send]]

delete protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast capability orf

show protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы
         address-family {
            ipv6-unicast {
               capability {
                  orf {
                     prefix-list {
                        receive
                        send
                     }
                  }
               }
            }
         }
      }
   }
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

receive

Возможность получения ORF от группы узлов.

send

Возможность отправки ORF в группу узлов.

Значение по умолчанию

Пиринговая сессия функционирует с минимальными возможностями.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для объявления поддержки ORF.

Форма **delete** этой команды используется для отказа возможности использования ORF.

Форма **show** этой команды используется для просмотра настройки конфигурации.

28.2.7 protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast default-originate

Разрешение пересылки маршрута по умолчанию группе узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast default-originate [route-map <имя_карты_маршрутов>]

delete protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast default-originate [route-map <имя_карты_маршрутов>]

show protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast default-originate
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы
         address-family {
            ipv6-unicast {
               default-originate {
                  route-map имя_карты_маршрутов
               }
            }
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

имя_карты_маршрутов

Указание настроенной карты маршрута, которая будет использоваться при объявлении маршрута по умолчанию.

Значение по умолчанию

По умолчанию пересылка маршрута запрещена.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для разрешения локальному маршрутизатору объявлять маршрут по умолчанию ::/0 группе узлов. Данный маршрут используется при невозможности использования других маршрутов. Маршрут::/0 не должен быть явно сконфигурирован на локальном маршрутизаторе. Для настройки карты маршрутов используется команда **protocols bgp <номер_AC> peer-group <имя_группы> local-as <номер_локальной_AC>**.

Форма **delete** этой команды используется для отключения переадресации маршрута по умолчанию или удаления карты маршрута.

Форма **show** этой команды используется для просмотра маршрута по умолчанию группы узлов.

28.2.8 protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast disable-send-community

Запрещение отправки расширенных атрибутов к указанной группе узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast disable-send-community [extended|standard]

delete protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast disable-send-community

show protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы
         address-family {
            ipv6-unicast {
               disable-send-community {
                  extended
                  standard
               }
            }
```

```
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

extended

Запрещение отправки расширенных атрибутов.

standard

Запрещение отправки стандартных атрибутов.

Значение по умолчанию

Отправка атрибутов по умолчанию разрешена.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для настройки запрещает отправку расширенных атрибутов по умолчанию.

Форма **delete** этой команды используется для восстановления настройки по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.2.9 protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast distribute-list export <список_доступа>

Применение списка доступа для фильтрации исходящих обновлений маршрутизации к группе узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast distribute-list export <список_доступа>

delete protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast distribute-list export

show protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast distribute-list export
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        peer-group имя_группы
            address-family {
                ipv6-unicast {
                    distribute-list {
                        export список_доступа
```

```
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

список_доступа

Номер стандартного или расширенного списка доступа. Диапазон для стандартного списка доступа равняется 1 - 99. Диапазон для расширенного списка доступа равняется 100 - 199.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для применения списка доступа для фильтрации исходящих обновлений маршрутизации к группе узлов.

Форма **delete** этой команды используется для отключения распространения списка доступа для фильтрации исходящих обновлений маршрутизации к группе узлов.

Форма **show** этой команды используется для просмотра настройки.

28.2.10 protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast distribute-list import <список_доступа>

Применение списка доступа для фильтрации входящих обновлений маршрутизации от группы узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast distribute-list import <список_доступа>

delete protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast distribute-list import

show protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast distribute-list import
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp <номер_AC> {
        peer-group <имя_группы> {
            address-family {
                ipv6-unicast {
                    distribute-list {
```

```
                    import <список_доступа>
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

имя_группы

Множественный узел. Название группы узлов.

список_доступа

Число стандартного или расширенного списка доступа. Диапазон для стандартного списка доступа равняется 1 - 99. Диапазон для расширенного списка доступа равняется 100 - 199.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для применения списка доступа для фильтрации входящих обновлений маршрутизации от группы узлов.

Форма **delete** этой команды используется для отключения распространения списка доступа для фильтрации входящих обновлений маршрутизации от группы узлов.

Форма **show** этой команды используется для просмотра настройки.

28.2.11 protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast filter-list export <имя_списка_путей>

Применение список пути AS к маршрутным обновлениям до указанной группы узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast filter-list export  <имя_списка_путей>

delete protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast filter-list export <имя_списка_путей>

show protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp <номер_AC> {
        peer-group <имя_группы> {
            address-family {
                ipv6-unicast {
                    filter-list {
```

```
                    export <имя_списка_путей>
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

имя_группы

Множественный узел. Название группы узлов.

имя_списка_путей

Имя списка путей для фильтрации обновлений маршрутов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для применения списка доступа для фильтрации исходящих обновлений маршрутизации.

Форма **delete** этой команды используется для отключения исходящих обновлений маршрутизации.

Форма **show** этой команды используется для просмотра настройки.

28.2.12 protocols bgp <номер_AC> peer-group <group-name> address-family ipv6-unicast filter-list import <имя_списка_путей>

Применение список пути AS к маршрутным обновлениям от указанной группы узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast filter-list import <имя_списка_путей>

delete protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast filter-list import <имя_списка_путей>

show protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast filter-list
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        peer-group имя_группы {
            address-family {
                ipv6-unicast {
                    filter-list {
                        import имя_списка_путей
                    }
```

```
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

<имя_группы>

Множественный узел. Название группы узлов.

<имя_списка_путей>

Имя списка путей для фильтрации обновлений маршрутов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для применения списка доступа для фильтрации входящих обновлений маршрутизации.

Форма **delete** этой команды используется для отключения входящих обновлений маршрутизации.

Форма **show** этой команды используется для просмотра настройки.

28.2.13 protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast maximum-prefix <число_префиксов>

Установка максимального числа префиксов, принимаемых группой узлов перед тем как она будет переведена в нерабочее состояние.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast maximum-prefix <число_префиксов>

delete protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast maximum-prefix <число_префиксов>

show protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        peer-group имя_группы {
            address-family {
                ipv6-unicast {
                    maximum-prefix число_префиксов
                }
            }
```

```
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

число_префиксов

Обязательный. Максимальное число префиксов, принимаемых группой узлов перед тем как она будет переведена в нерабочее состояние.

Значение по умолчанию

Максимальное число префиксов не указывается.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для установки максимального числа префиксов.

Форма **delete** этой команды используется для удаления настройки.

Форма **show** этой команды используется для просмотра настройки.

28.2.14 protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast nexthop-local unchanged

Указание IPv6-адреса, не изменяемого при анонсировании префикса узлом.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast nexthop-local unchanged

delete protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast nexthop-local

show protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast nexthop-local
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        peer-group имя_группы {
            address-family {
                ipv6-unicast {
                    nexthop-local {
                        unchanged
                    }
                }
            }
```

```
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

Значение по умолчанию

IPv6-адрес не меняется при анонсировании префикса узлом.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для указания IPv6-адреса, не изменяемого при анонсировании префикса узлом.

Форма **delete** этой команды используется для восстановления настроек по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.2.15 protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast nexthop-self

Установка локального маршрутизатора как следующего транзитного узла для группы узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast nexthop-self

delete protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast nexthop-self

show protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        peer-group имя_группы {
            address-family {
                ipv6-unicast {
                    nexthop-self
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

Значение по умолчанию

Запрещено.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для установки локального маршрутизатора как следующего транзитного узла для группы узлов.

Форма **delete** этой команды используется для удаления настройки.

Форма **show** этой команды используется для просмотра настройки.

28.2.16 protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast prefix-list export <имя_префикс-листа>

Применение префиксного списка для фильтрации обновлений к группе узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast prefix-list export <имя_префикс-листа>

delete protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast prefix-list export <имя_префикс-листа>

show protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast prefix-list
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        peer-group имя_группы {
            address-family {
                ipv6-unicast {
                    prefix-list {
                        export имя_префикс-листа
                    }
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

имя_префикс-листа

Название сконфигурированного префиксного списка.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для ограничения распространения исходящей информации о группе узлов используя фильтрование с помощью префиксного списка.

Форма **delete** этой команды используется для удаления префиксного фильтра.

Форма **show** этой команды используется для просмотра настройки.

28.2.17 protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast prefix-list import <имя_префикс-листа>

Применение префиксного списка для фильтрации обновлений от группы узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast prefix-list import <имя_префикс-листа>

delete protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast prefix-list import <имя_префикс-листа>

show protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast prefix-list
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        peer-group имя_группы {
            address-family {
                ipv6-unicast {
                    prefix-list {
                        import имя_префикс-листа
                    }
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

имя_префикс-листа

Название сконфигурированного префиксного списка.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для ограничения распространения входящей информации о группе узлов используя фильтрование с помощью префиксного списка.

Форма **delete** этой команды используется для удаления префиксного фильтра.

Форма **show** этой команды используется для просмотра настройки.

28.2.18 protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast remove-private-as

Предписание локальному маршрутизатору на исключение частных AC от обновлений.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast remove-private-as

delete protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast remove-private-as

show protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        peer-group имя_группы {
            address-family {
                ipv6-unicast {
                    remove-private-as
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

Значение по умолчанию

Частные AC включены в исходящие обновления.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для указания локальному маршрутизатору об исключении частных AC от обновлений. При активации данной функции, маршрутизатор отпускает частные AC от атрибута AS_PATH. Команда может использоваться в конфедерациях при условии, что частные AS добавлены после части конфедерации пути AS. Данная команда применяется только к узлам eBGP; и не может использоваться с узлами iBGP.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.2.19 protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast route-map export <имя_карты_маршрутов>

Применение карты маршрута для фильтрации обновлений к группе узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast route-map export <имя_карты_маршрутов>

delete protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast route-map export <имя_карты_маршрутов>

show protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast route-map export
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        peer-group имя_группы {
            address-family {
                ipv6-unicast {
                    route-map {
                        export имя_карты_маршрутов
                    }
                }
            }
        }
    }
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных АС.

имя_группы

Множественный узел. Название группы узлов.

имя_карты_маршрутов

Указание настроенной карты маршрута, которая будет использоваться при объявлении маршрута по умолчанию.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для ограничения распределение исходящей информации о группе узлов используя фильтрацию карты маршрута.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.2.20 protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast route-map import <имя_карты_маршрутов>

Применение карты маршрута для фильтрации обновлений от группы узлов.

Синтаксис

```
set protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast route-map import <имя_карты_маршрутов>

delete protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast route-map import <имя_карты_маршрутов>

show protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast route-map import
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_АС {
        peer-group имя_группы {
            address-family {
                ipv6-unicast {
                    route-map {
                        import имя_карты_маршрутов
                    }
                }
            }
        }
    }
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных АС.

имя_группы

Множественный узел. Название группы узлов.

имя_карты_маршрутов

Указание настроенной карты маршрута, которая будет использоваться при объявлении маршрута по умолчанию.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для ограничения распределение входящей информации о группе узлов используя фильтрацию карты маршрута.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.2.21 protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast soft-reconfiguration inbound

Предписание локальному маршрутизатору на сохранение полученных маршрутных обновлений.

Синтаксис

```
set protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast soft-reconfiguration inbound

delete protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast soft-reconfiguration inbound

show protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_АС {
      peer-group имя_группы {
         address-family {
            ipv6-unicast {
               soft-reconfiguration {
                  inbound
               }
            }
         }
      }
   }
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных АС.

имя_группы

Множественный узел. Название группы узлов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для включения режима мягкого реконфигурирования, при котором локальный маршрутизатор сохраняет маршрутные обновления.

Форма **delete** этой команды используется для отключения мягкого реконфигурирования.

Форма **show** этой команды используется для просмотра настройки.

28.2.22 protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast unsuppress-map <имя_карты_маршрутов>

Предписание локальному маршрутизатору выборочно распространять маршруты на основе маршрутной карты.

Синтаксис

```
set protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast unsuppress-map <имя_карты_маршрутов>

delete protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast unsuppress-map <имя_карты_маршрутов>

show protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_АС {
        peer-group имя_группы {
            address-family {
                ipv6-unicast {
                    unsuppress-map имя_карты_маршрутов
                }
            }
        }
    }
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных АС.

имя_группы

Множественный узел. Название группы узлов.

имя_карты_маршрутов

Указание настроенной карты маршрута, которая будет использоваться при объявлении маршрута по умолчанию.

Значение по умолчанию

Маршруты не распространяются.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для выборочного распространения маршрутов.

Форма **delete** этой команды используется для восстановления настроек по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.2.23 protocols bgp <номер_AC> peer-group <имя_группы> allowas-in

Разрешение на получение объявления, содержащего атрибут AS_PATH локальному маршрутизатору.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> allowas-in [number <количество>]
delete protocols bgp <номер_AC> peer-group <имя_группы> allowas-in
show protocols bgp <номер_AC> peer-group <имя_группы>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы {
         allowas-in {
            number количество
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой АС при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных АС.

имя_группы

Множественный узел. Название группы узлов.

количество

Количество попыток на получение объявления, атрибута AS_PATH локальному маршрутизатору. Диапазон составляет от 1 до 10 попыток.

Значение по умолчанию

Получение объявления атрибута AS_PATH запрещено.

Указания по использованию

Форма **set** этой команды используется для разрешения локальному маршрутизатору принимать объявления атрибута AS_PATH.

Форма **delete** этой команды используется для запрещения локальному маршрутизатору принимать объявления атрибута AS_PATH.

Форма **show** этой команды используется для просмотра настройки конфигурации.

28.2.24 protocols bgp <номер_AC> peer-group <имя_группы> attribute-unchanged

Разрешение локальному маршрутизатору передачи обновлений группе узлов с неизменными атрибутами.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> attribute-unchanged [as-path|med|next-hop]

delete protocols bgp <номер_AC> peer-group <имя_группы> attribute-unchanged [as-path|med|next-hop]

show protocols bgp <номер_AC> peer-group <имя_группы> attribute-unchanged
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        peer-group имя_группы {
            attribute-unchanged {
                as-path
                med
                next-hop
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

as-path

Распространяет маршрутное обновление с неизменным атрибутом AS_PATH.

med

Маршрутное обновление с неизменным атрибутом AS_PATH.

next-hop

Маршрутное обновление с неизменным атрибутом next-hop.

Значение по умолчанию

Запрещено.

Указания по использованию

Форма **set** этой команды используется для разрешения передачи локальным маршрутизатором обновлений маршрутов, без изменения атрибутов BGP: AS_PATH, MED и next-hop.

Форма **delete** этой команды используется для восстановления нормальной модификации атрибутов BGP.

Форма **show** этой команды используется для просмотра настройки конфигурации.

28.2.25 protocols bgp <номер_AC> peer-group <имя_группы> capability dynamic

Объявление поддержки динамического обновления, получаемого от группы узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> capability dynamic
delete protocols bgp <номер_AC> peer-group <имя_группы> capability dynamic
show protocols bgp <номер_AC> peer-group <имя_группы> capability
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы {
         capability {
            dynamic
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

Значение по умолчанию

Пиринговая сессия функционирует с минимальными возможностями.

Указания по использованию

Форма **set** этой команды используется для объявления поддержки динамического обновления, получаемого от группы узлов, без изменения атрибутов BGP: AS_PATH, MED и next-hop.

Форма **delete** этой команды используется для отказа возможности динамического обновления.

Форма **show** этой команды используется для просмотра настройки конфигурации.

28.2.26 protocols bgp <номер_AC> peer-group <имя_группы> capability orf

Объявление поддержки Outbound Route Filtering (ORF), получаемого от группы узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> capability orf [prefix-list [receive | send]]

delete protocols bgp <номер_AC> peer-group <имя_группы> capability orf

show protocols bgp <номер_AC> peer-group <имя_группы> capability
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы {
         capability {
            orf {
               prefix-list {
                  receive
                  send
               }
            }
         }
      }   }}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

prefix-list

Распространение префиксного списка ORF к группе узлов.

receive

Возможность получения ORF от группы узлов.

send

Возможность отправки ORF в группу узлов.

Значение по умолчанию

Пиринговая сессия функционирует с минимальными возможностями.

Указания по использованию

Форма **set** этой команды используется для объявления поддержки ORF.

Форма **delete** этой команды используется для отказа возможности использования ORF.

Форма **show** этой команды используется для просмотра настройки конфигурации.

28.2.27 protocols bgp <номер_AC> peer-group <имя_группы> default-originate

Разрешение пересылки маршрута по умолчанию группе узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> default-originate [route-map <имя_карты_маршрутов>]

delete protocols bgp <номер_AC> peer-group <имя_группы> default-originate [route-map <имя_карты_маршрутов>]

show protocols bgp <номер_AC> peer-group <имя_группы> default-originate
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        peer-group имя_группы {
            default-originate {
                route-map имя_карты_маршрутов
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

имя_карты_маршрутов

Указание настроенной карты маршрута, которая будет использоваться при объявлении маршрута по умолчанию.

Значение по умолчанию

По умолчанию пересылка маршрута запрещена.

Указания по использованию

Форма **set** этой команды используется для разрешения локальному маршрутизатору объявлять маршрут по умолчанию ::/0 группе узлов. Данный маршрут используется при невозможности использования других маршрутов. Маршрут::/0 не должен быть явно сконфигурирован на локальном маршрутизаторе. Для настройки карты маршрутов используется команда **protocols bgp <номер_AC> peer-group <group-name> local-as <номер_AC>**.

Форма **delete** этой команды используется для отключения переадресации маршрута по умолчанию или удаления карты маршрута.

Форма **show** этой команды используется для просмотра маршрута по умолчанию группы узлов.

28.2.28 protocols bgp <номер_AC> peer-group <имя_группы> description <описание>

Краткое описание группы узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> description <описание>
delete protocols bgp <номер_AC> peer-group <имя_группы> description
show protocols bgp <номер_AC> peer-group <имя_группы>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы {
         description описание      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

описание

Описание (до 80 симолов) группы узлов. В случае использования пробелов, описание должно быть заключено в кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для краткого описания группы узлов.

Форма **delete** этой команды используется для удаления краткого описания группы узлов.

Форма **show** этой команды используется для просмотра настройки.

28.2.29 protocols bgp <номер_AC> peer-group <имя_группы> disable-capability-negotiation

Отключение согласования возможностей BGP.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> disable-capability-negotiation
delete protocols bgp <номер_AC> peer-group <имя_группы> disable-capability-negotiation
show protocols bgp <номер_AC> peer-group <имя_группы>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
```

```
        peer-group имя_группы {
            disable-capability-negotiation
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

Значение по умолчанию

Согласования возможностей BGP выполняется.

Указания по использованию

Форма **set** этой команды используется для отключения согласования возможностей BGP

Форма **delete** этой команды используется для удаления этого атрибута и восстановления согласования возможностей BGP.

Форма **show** этой команды используется для просмотра настройки.

28.2.30 protocols bgp <номер_AC> peer-group <имя_группы> disable-connected-check

Отключение проверки прямого подключения для транзитного узла.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> disable-connected-check
delete protocols bgp <номер_AC> peer-group <имя_группы> disable-connected-check
show protocols bgp <номер_AC> peer-group <имя_группы>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        peer-group имя_группы {
            disable-connected-check
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

Значение по умолчанию

Проверка соединения выполняется.

Указания по использованию

Форма **set** этой команды используется для отключения проверки соединения для транзитного узла.

Форма **delete** этой команды используется для восстановления проверки соединения для транзитного узла.

Форма **show** этой команды используется для просмотра настройки.

28.2.31 protocols bgp <номер_AC> peer-group <имя_группы> disable-send-community

Запрещение отправки расширенных атрибутов к указанной группе узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> disable-send-community [extended | standard]

delete protocols bgp <номер_AC> peer-group <имя_группы> disable-send-community

show protocols bgp <номер_AC> peer-group <имя_группы>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы {
         disable-send-community {
            extended
            standard
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой АС при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных АС.

имя_группы

Множественный узел. Название группы узлов.

extended

Запрещение отправки расширенных атрибутов.

standard

Запрещение отправки стандартных атрибутов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для настройки запрещает отправку расширенных атрибутов по умолчанию.

Форма **delete** этой команды используется для восстановления настройки по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.2.32 protocols bgp <номер_AC> peer-group <имя_группы> distribute-list export <список_доступа>

Применение списка допуска, для фильтрации исходящих маршрутных обновлений группы узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> distribute-list export <список_доступа>

delete protocols bgp <номер_AC> peer-group <имя_группы> distribute-list

show protocols bgp <номер_AC> peer-group <имя_группы> distribute-list
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы {
         distribute-list {
            export список_доступа
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

список_доступа

Число стандартного или расширенного списка доступа. Диапазон для стандартного списка доступа равняется 1 - 99. Диапазон для расширенного списка доступа равняется 100 - 199.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для применения списка допуска, для фильтрации исходящих маршрутных обновлений группы узлов.

Форма **delete** этой команды используется для восстановления настройки по умолчанию.

Форма **show** этой команды используется для просмотра настройки конфигурации BGP соседа.

28.2.33 protocols bgp <номер_AC> peer-group <имя_группы> distribute-list import <список_доступа>

Применение списка допуска, для фильтрации входящих маршрутных обновлений группы узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> distribute-list import <список_доступа>

delete protocols bgp <номер_AC> peer-group <имя_группы> distribute-list

show protocols bgp <номер_AC> peer-group <имя_группы> distribute-list
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы {
         distribute-list {
            import список_доступа
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

список_доступа

Число стандартного или расширенного списка доступа. Диапазон для стандартного списка доступа равняется 1 - 99. Диапазон для расширенного списка доступа равняется 100 - 199.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для применения списка допуска, для фильтрации входящих маршрутных обновлений группы узлов.

Форма **delete** этой команды используется для восстановления настройки по умолчанию.

Форма **show** этой команды используется для просмотра настройки конфигурации BGP соседа.

28.2.34 protocols bgp <номер_AC> peer-group <имя_группы> ebgp-multihop <количество_переходов>

Предоставление участия в динамической маршрутизации узлам, не соединенным напрямую.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> ebgp-multihop <количество_переходов>
```

```
delete protocols bgp <номер_AC> peer-group <имя_группы> ebgp-multihop
show protocols bgp  <номер_AC> peer-group <имя_группы>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы {
         ebgp-multihop количество_переходов
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

количество_переходов

Время жизни или максимальное количество возможных транзитных участков. Диапазон 1 — 255.

Значение по умолчанию

Участие в динамической маршрутизации возможно только узлам соединенным напрямую.

Указания по использованию

Форма **set** этой команды используется для предоставления участия в динамической маршрутизации узлам, не соединенным напрямую.

Форма **delete** этой команды используется для восстановления настройки по умолчанию.

Форма **show** этой команды используется для просмотра настройки конфигурации BGP соседа.

28.2.35 protocols bgp <номер_AC> peer-group <имя_группы> filter-list export <имя_списка_путей>

Применение список пути AS к маршрутным обновлениям до указанной группы узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> filter-list export
<имя_списка_путей>
delete protocols bgp <номер_AC> peer-group <имя_группы> filter-list export
<имя_списка_путей>
show protocols bgp <номер_AC> peer-group <имя_группы> filter-list
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы {
```

```
            filter-list {
                export <имя_списка_путей>
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

имя_списка_путей

Имя списка путей для фильтрации обновлений маршрутов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для применения списка доступа для фильтрации исходящих обновлений маршрутизации.

Форма **delete** этой команды используется для отключения исходящих обновлений маршрутизации.

Форма **show** этой команды используется для просмотра настройки.

28.2.36 protocols bgp <номер_AC> peer-group <имя_группы> filter-list import <имя_списка_путей>

Применение список пути AS к маршрутным обновлениям до указанной группы узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> filter-list import <имя_списка_путей>

delete protocols bgp <номер_AC> peer-group <имя_группы> filter-list import <имя_списка_путей>

show protocols bgp <номер_AC> peer-group <имя_группы> filter-list
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        peer-group имя_группы {
            filter-list {
                import имя_списка_путей
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

имя_списка_путей

Имя списка путей для фильтрации обновлений маршрутов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для применения списка доступа для фильтрации входящих обновлений маршрутизации.

Форма **delete** этой команды используется для отключения входящих обновлений маршрутизации.

Форма **show** этой команды используется для просмотра настройки.

28.2.37 protocols bgp <номер_AC> peer-group <имя_группы> local-as <номер_локальной_AC>

Указание номера локальной AC для равноправных узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> local-as <номер_локальной_AC> [no-prepend]

delete protocols bgp <номер_AC> peer-group <имя_группы> local-as <номер_локальной_AC> [no-prepend]

show protocols bgp <номер_AC> peer-group <имя_группы> local-as
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы {
         local-as номер_локальной_AC {
            no-prepend
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

номер_локальной_АС

Допустимый номер АС. Нельзя использовать номер АС, которому принадлежит группа узлов. Значение должно лежать в диапазоне от 1 до 4294967294.

no-prepend

Указание маршрутизатору не ожидать номер локальной АС к маршрутам, полученным от внешнего узла.

Значение по умолчанию

Отсутствует.

Указания по использованию

Локальный номер автономной системы может только быть применен к eBGP коллегам; не может быть применено к коллегам в различных подавтономных системах в конфедерации.

Форма **set** этой команды используется для указания номера локальной АС для равноправных узлов. Данный номер используется всеми членами группы узлов при взаимодействии.

Форма **delete** этой команды используется для удаления номера локальной АС.

Форма **show** этой команды используется для просмотра настройки.

28.2.38 protocols bgp <номер_АС> peer-group <имя_группы> maximum-prefix <число_префиксов>

Установка максимального числа префиксов, принимаемых группой узлов перед тем как она будет переведена в нерабочее состояние.

Синтаксис

```
set protocols bgp <номер_АС> peer-group <имя_группы> maximum-prefix <число_префиксов>

delete protocols bgp <номер_АС> peer-group <имя_группы> maximum-prefix <число_префиксов>

show protocols bgp <номер_АС> peer-group <имя_группы>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_АС {
        peer-group имя_группы {
            maximum-prefix число_префиксов
        }
    }
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных АС.

имя_группы

Множественный узел. Название группы узлов.

число_префиксов

Максимальное число префиксов, принимаемых группой узлов перед тем как она будет переведена в нерабочее состояние.

Значение по умолчанию

Максимальное число префиксов не указывается.

Указания по использованию

Форма **set** этой команды используется для установки максимального числа префиксов.

Форма **delete** этой команды используется для удаления настройки.

Форма **show** этой команды используется для просмотра настройки.

28.2.39 protocols bgp <номер_AC> peer-group <group-name> nexthop-self

Установка локального маршрутизатора как следующего транзитного участка для группы узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> nexthop-self
delete protocols bgp <номер_AC> peer-group <имя_группы> nexthop-self
show protocols bgp <номер_AC> peer-group <имя_группы>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы {
         nexthop-self
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

Значение по умолчанию

Запрещено.

Указания по использованию

Форма **set** этой команды используется для установки локального маршрутизатора как следующего транзитного участка для группы узлов.

Форма **delete** этой команды используется для удаления настройки.

Форма **show** этой команды используется для просмотра настройки.

28.2.40 protocols bgp <номер_AC> peer-group <имя_группы> override-capability

Разрешение на пиринговую сессию с группой узлов, которая не поддерживает согласование возможностей.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> override-capability
```

```
delete protocols bgp <номер_AC> peer-group <имя_группы> override-capability
show protocols bgp <номер_AC> peer-group <имя_группы>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы {
         override-capability
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

Значение по умолчанию

Пиринговая сессия не может быть установлена, если группа узлов не поддерживает согласование возможностей.

Указания по использованию

Форма **set** этой команды используется для для разрешения пиринговой сессии с группой узлов, которая не поддерживает согласование возможностей. Как правило, если узел не поддерживает согласование возможностей, пиринговая сессия не может быть установлена.

Форма **delete** этой команды используется для восстановления настройки по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.2.41 protocols bgp <номер_AC> peer-group <имя_группы> passive

Предписание маршрутизатору не инициировать соединение указанной группой узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> passive
delete protocols bgp <номер_AC> peer-group <имя_группы> passive
show protocols bgp <номер_AC> peer-group <имя_группы>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы {
         passive
      }
   }
```

```
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных АС.

имя_группы

Множественный узел. Название группы узлов.

Значение по умолчанию

Маршрутизатор принимает входящие соединения и инициирует исходящие соединения.

Указания по использованию

Форма **set** этой команды используется для настройки маршрутизатора таким образом, чтобы осуществлялся прием входящих сообщений от группы узлов, но в то же время не происходило инициализации исходящих сообщений.

Форма **delete** этой команды используется для восстановления настройки по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.2.42 protocols bgp <номер_АС> peer-group <имя_группы> password <пароль>

Указание хешированного в MD5 пароля.

Синтаксис

```
set protocols bgp <номер_АС> peer-group <имя_группы> password <пароль>
delete protocols bgp <номер_АС> peer-group <имя_группы> password
show protocols bgp <номер_АС> peer-group <имя_группы> password
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_АС {
      peer-group имя_группы {
         password пароль
      }
   }
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных АС.

имя_группы

Множественный узел. Название группы узлов.

пароль

Пароль, хешированный в MD5.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания пароля и его последующего хеширования в MD5.

Форма **set** этой команды используется для указания хешированного в MD5 пароля.

Форма **delete** этой команды используется для удаления настройки.

Форма **show** этой команды используется для просмотра настройки конфигурации BGP соседа.

28.2.43 protocols bgp <номер_AC> peer-group <имя_группы> prefix-list export <имя_префикс-листа>

Применение префиксного списка для фильтрации обновлений к группе узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> prefix-list export <имя_префикс-листа>

delete protocols bgp <номер_AC> peer-group <имя_группы> prefix-list export <имя_префикс-листа>

show protocols bgp <номер_AC> peer-group <имя_группы> prefix-list
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы {
         prefix-list {
            export имя_префикс-листа
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

имя_префикс-листа

Название сконфигурированного префиксного списка.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для ограничения распространения исходящей информации о группе узлов используя фильтрование с помощью префиксного списка.

Форма **delete** этой команды используется для удаления префиксного фильтра.

Форма **show** этой команды используется для просмотра настройки.

28.2.44 protocols bgp <номер_AC> peer-group <имя_группы> prefix-list import <имя_префикс-листа>

Применение префиксного списка для фильтрации обновлений от группы узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> prefix-list import <имя_префикс-листа>

delete protocols bgp <номер_AC> peer-group <имя_группы> prefix-list import <имя_префикс-листа>

show protocols bgp <номер_AC> peer-group <имя_группы> prefix-list
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        peer-group имя_группы {
            prefix-list {
                import имя_префикс-листа
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

имя_префикс-листа

Название сконфигурированного префиксного списка.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для ограничения распространения входящей информации о группе узлов используя фильтрование с помощью префиксного списка.

Форма **delete** этой команды используется для удаления префиксного фильтра.

Форма **show** этой команды используется для просмотра настройки.

28.2.45 protocols bgp <номер_AC> peer-group <имя_группы> remote-as <номер_удаленной_AC>

Указание маршрутизатору на удаление частных AC из обновлений, отправленных на указанную группу узлов.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> remote-as <номер_удаленной_AC>
```

```
delete protocols bgp <номер_AC> peer-group <имя_группы> remote-as
show protocols bgp <номер_AC> peer-group <имя_группы>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы {
         remote-as номер_удаленной_AC
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

номер_удаленной_AC

Допустимый номер AC. Нельзя использовать номер AC, которому принадлежит группа узлов. Значение должно лежать в диапазоне от 1 до 4294967294.

Значение по умолчанию

Частные AC включены в исходящие обновления.

Указания по использованию

Эта команда применяется только к коллегам eBGP; это не может использоваться с коллегами iBGP.

Форма **set** этой команды используется для указания маршрутизатору на удаление частных AC из обновлений, отправленных на указанную группу узлов. При активации данной опции, маршрутизатор при обновлении пропускает частные AC. Диапазон номеров для частных AC варьируется от 64512 до 65534.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.2.46 protocols bgp <номер_AC> peer-group <имя_группы> remove-private-as

Предписание локальному маршрутизатору на исключение частных AC от обновлений.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> remove-private-as
delete protocols bgp <номер_AC> peer-group <имя_группы> remove-private-as
show protocols bgp <номер_AC> peer-group <имя_группы>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы {
```

```
            remove-private-as
        }
    }
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных АС.

имя_группы

Множественный узел. Название группы узлов.

Значение по умолчанию

Частные АС включены в исходящие обновления.

Указания по использованию

Форма **set** этой команды используется для указания локальному маршрутизатору об исключении частных AS от обновлений. При активации данной функции, маршрутизатор отпускает частные АС от атрибута AS_PATH. Команда может использоваться в конфедерациях при условии, что частные AS добавлены после части конфедерации пути AS. Данная команда применяется только к узлам eBGP; и не может использоваться с узлами iBGP.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.2.47 protocols bgp <номер_АС> peer-group <имя_группы> shutdown

Административное прекращение работы группы узлов.

Синтаксис

```
set protocols bgp <номер_АС> peer-group <имя_группы> shutdown
delete protocols bgp <номер_АС> peer-group <имя_группы> shutdown
show protocols bgp <номер_АС> peer-group <имя_группы>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_АС {
        peer-group имя_группы {
            shutdown
        }
    }
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных АС.

имя_группы

Множественный узел. Название группы узлов.

Значение по умолчанию

Отключено.

Указания по использованию

Форма **set** этой команды используется для административного прекращения работы группы узлов. Прекращение работы маршрутизатора завершает любые активные сеансы группы узлов и удаляет любую связанную маршрутную информацию.

Форма **delete** этой команды используется для повторного начала работы группы узлов.

Форма **show** этой команды используется для просмотра настройки.

28.2.48 protocols bgp <номер_AC> peer-group <имя_группы> soft-reconfiguration inbound

Установить перенастройку без сброса соединений для данной группы узлов

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> soft-reconfiguration inbound

delete protocols bgp <номер_AC> peer-group <имя_группы> soft-reconfiguration inbound

show protocols bgp <номер_AC> peer-group <имя_группы>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        peer-group имя_группы {
            soft-reconfiguration {
                inbound
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для включения режима мягкого реконфигурирования, при котором локальный маршрутизатор сохраняет маршрутные обновления.

Форма **delete** этой команды используется для отключения мягкого реконфигурирования.

Форма **show** этой команды используется для просмотра настройки.

28.2.49 protocols bgp <номер_AC> peer-group <имя_группы> ttl-security hops <число_переходов>

Установка TTL для транзитных участков для указанной группы узлов

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> ttl-security hops <число_переходов>
delete protocols bgp <номер_AC> peer-group <имя_группы> ttl-security hops
show protocols bgp <номер_AC> peer-group <имя_группы> ttl-security hops
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы {
         ttl-security {
            hops число_переходов
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

число_переходов

Максимальное количество принятых на время пиринговой сессии транзитных участков от локальной узла. Значение должно лежать в диапазоне от 1 до 254.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для определения числа транзитных участков.

Форма **delete** этой команды используется для восстановления настроек по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.2.50 protocols bgp <номер_AC> peer-group <имя_группы> unsuppress-map <имя_карты_маршрутов>

Предписание локальному маршрутизатору выборочно распространять маршруты на основе маршрутной карты.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> unsuppress-map <имя_карты_маршрутов>
```

```
delete protocols bgp <номер_AC> peer-group <имя_группы> unsuppress-map
<имя_карты_маршрутов>

show protocols <номер_AC> peer-group <имя_группы> unsuppress-map
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы {
         unsuppress-map имя_карты_маршрутов
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

имя_группы

Множественный узел. Название группы узлов.

имя_карты_маршрутов

Указание настроенной карты маршрута, которая будет использоваться при объявлении маршрута по умолчанию.

Значение по умолчанию

Маршруты не распространяются.

Указания по использованию

Форма **set** этой команды используется для выборочного распространения маршрутов.

Форма **delete** этой команды используется для восстановления настроек по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.2.51 protocols bgp <номер_AC> peer-group <имя_группы> update-source

Определение исходного IP-адреса или интерфейса маршрутных обновлений.

Синтаксис

```
set protocols bgp <номер_AC> peer-group <имя_группы> update-source [<адрес> |
<интерфейс>]

delete protocols bgp <номер_AC> peer-group <имя_группы> update-source

show protocols bgp <номер_AC> peer-group <имя_группы>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      peer-group имя_группы {
         update-source адрес | интерфейс
```

```
        }
    }
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных АС.

имя_группы

Множественный узел. Название группы узлов.

адрес

IPv4-адрес маршрутизатора откуда поступают маршрутные обновления.

интерфейс

Интерфейс маршрутизатора откуда поступают маршрутные обновления.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для настройки системы получать маршрутные обновления из определенного источника.

Форма **delete** этой команды используется для удаления настройки.

Форма **show** этой команды используется для просмотра настройки.

28.2.52 protocols bgp <номер_АС> peer-group <имя_группы> weight <вес>

Определение веса по умолчанию для маршрутов от группы узлов.

Синтаксис

```
set protocols bgp <номер_АС> peer-group <имя_группы> weight <вес>
delete protocols bgp <номер_АС> peer-group <имя_группы> weight
show protocols bgp <номер_АС> peer-group <имя_группы>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_АС {
        peer-group имя_группы {
            weight вес
        }
    }
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных АС.

имя_группы

Множественный узел. Название группы узлов.

вес

Вес который присваивается маршрутам от указанной группы узлов. Значение должно лежать в диапазоне от 0 до 65535.

Значение по умолчанию

Маршруты получаемые от узла имеют вес равный 0. Маршруты получаемые от локального маршрутизатора имеют вес равный 32768.

Указания по использованию

Эта команда используется для настройки IPv6 одноадресных маршрутов.

Форма **set** этой команды используется для установки значения весов маршрутов.

Форма **delete** этой команды используется для восстановления настроек по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.2.53 clear ip bgp peer-group <group-name>

Сброс пиринговой сессии для всех членов группы узлов.

Синтаксис

```
clear ip bgp peer-group <имя_группы> [in [prefix-filter] | out | soft [in | out]]
```

Режим ввода команды

Эксплуатационный режим.

Параметры

имя_группы

Множественный узел. Название группы узлов.

in

Очистить все узлы в группе с помощью мягкого переконфигурирования входных обновлений протокола bgp.

out

Очистить все узлы в группе с помощью мягкого переконфигурирования исходящих обновлений протокола bgp.

prefix-filter

Очистить все списки префиксов с помощью мягкого переконфигурирования входных обновлений протокола bgp

soft

Очистить все узлы в группе с помощью мягкого переконфигурирования протокола bgp

Значение по умолчанию

При использовании без параметра **soft**, входящие и исходящие соединения будут сброшены.

Указания по использованию

Данная команда используется для сброса пиринговой сессии для всех элементов группы узлов. При этом будут применены новые политики BGP. При использовании параметра **soft**, маршруты от узлов будут отмечены как устарелые, но не будут сразу удалены из таблицы BGP. Устаревшие маршруты, которые не получены от узлов будут удалены при восстановлении соединения.

28.2.54 clear ip bgp peer-group <group-name> ipv4 unicast

Сброс IPv4-сессии для всех членов группы узлов.

Синтаксис

```
clear ip bgp peer-group <имя_группы> ipv4 unicast [in [prefix-filter] | out | soft [in |out]]
```

Режим ввода команды

Эксплуатационный режим.

Параметры

имя_группы

Множественный узел. Название группы узлов.

in

Очистить информацию с помощью мягкого переконфигурирования входных обновлений протокола bgp

out

Очистить информацию с помощью мягкого переконфигурирования выходных обновлений протокола bgp

prefix-filter

Очистить списки префиксов и сделать мягкое переконфигурирование входных обновлений протокола bgp

soft

Очистить информацию с помощью мягкого переконфигурирования протокола bgp

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для сброса входящих одноадресатных сеансов для всех элементов группы узлов. При этом будут применены новые политики BGP.

28.3 Конфедерация автономных систем

Команды для настройки конфедераций автономных систем	
protocols bgp <номер_AC> parameters confederation identifier <идентификатор_AC>	Указание уникального номера (идентификатора, ID) автономной подсистеме, входящей в конфедерацию.
protocols bgp <номер_AC> parameters confederation peers <номер_соседней_AC>	Указание уникального номера для узлов, входящих в автономную подсистему конфедерации

28.3.1 protocols bgp <номер_AC> parameters confederation identifier <идентификатор_AC>

Указание идентификатора автономной подсистеме, входящей в конфедерацию.

Синтаксис

```
set protocols bgp <номер_AC> parameters confederation identifier <идентификатор_AC>

delete protocols bgp <номер_AC> parameters confederation identifier <идентификатор_AC>

show protocols bgp <номер_AC> parameters confederation
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      parameters {
         confederation {
```

```
            identifier идентификатор_AC
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

идентификатор_AC

Уникальный номер, являющийся идентификатором автономной подсистемы, входящей в конфедерацию. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных подсистем.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для указания идентификатора автономной подсистеме, входящей в конфедерацию.

Форма **delete** этой команды используется для удаления идентификатора автономной подсистемы, входящей в конфедерацию.

Форма **show** этой команды используется для просмотра настроек конфедерации.

28.3.2 protocols bgp <номер_AC> parameters confederation peers <номер_соседней_AC>

Указание уникального номера для узлов, входящих в автономную подсистему конфедерации.

Синтаксис

```
set protocols bgp <номер_AC> parameters confederation peers asn <номер_соседней_AC>
delete protocols bgp <номер_AC> parameters confederation peers asn <номер_соседней_AC>
show protocols bgp <номер_AC> parameters confederation peers asn
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        parameters {
            confederation {
                peers номер_соседней_AC
            }
        }
    }
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных АС.

номер_соседней_АС

Уникальный номер узла автономной подсистемы, входящей в конфедерацию. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для *локальных АС*. Множество узлов указываются в виде списка, разделенного пробелами.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для указания узлов автономной подсистемы, входящей в конфедерацию. Для узлов извне, данная конфедерация будет определяться как отдельная АС.

Форма **delete** этой команды используется для удаления узлов автономной подсистемы, входящей в конфедерацию.

Форма **show** этой команды используется для просмотра настроек конфедерации.

28.4 Настройка узлов BGP

Команды настройки узлов BGP	
protocols bgp <номер_АС> neighbor <идентификатор>	Указание узла BGP.
protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast	Определение конфигурации однонаправленных IPv6-маршрутов BGP для пиринговой сессии.
protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast allowas-in	Разрешение на получение объявления, содержащего атрибут AS_PATH локальному маршрутизатору.
protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast attribute-unchanged	Разрешение локальному маршрутизатору передачи обновлений узлу с неизменными атрибутами.
protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast capability dynamic	Объявление поддержки динамического обнвления, получаемого от узла.
protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast capability orf	Объявление поддержки Outbound Route Filtering (ORF), получаемого от узла .
protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast default-originate	Разрешение пересылки маршрута по умолчанию
protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast disable-send-community	Запрещение отправки расширенных атрибутов к указанному узлу.
protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast distribute-list export <список_доступа>	Применение списка доступа для фильтрации исходящих обновлений маршрутизации к узлу.
protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast distribute-list import <список_доступа>	Применение списка доступа для фильтрации входящих обновлений маршрутизации от узла.
protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast filter-list export <имя_списка_путей>	Применение списка пути AS к маршрутным обновлениям до указанного узла.
protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast filter-list import <имя_списка_путей>	Применение списка пути AS к маршрутным обновлениям от указанного узла.
protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast maximum-prefix <число_префиксов>	Установка максимального числа префиксов, принимаемых узлом перед тем, как он будет переведен в нерабочее состояние.

protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast nexthop-local unchanged	Указание IPv6-адреса, не изменяемого при анонсировании префикса узлом.
protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast nexthop-self	Установка локального маршрутизатора как следующего транзитного участка для узла.
protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast prefix-list export <имя_префикс-листа>	Применение префиксного списка для фильтрации обновлений к узлу.
protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast prefix-list import <имя_префикс-листа>	Применение префиксного списка для фильтрации обновлений от узла.
protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast remove-private-as	Предписание локальному маршрутизатору на исключение частных АС от обновлений.
protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast route-map export <имя_карты_маршрутов>	Применение карты маршрута для фильтрации обновлений к узлу.
protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast route-map import <имя_карты_маршрутов>	Применение карты маршрута для фильтрации обновлений от узла.
protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast soft-reconfiguration inbound	Предписание локальному маршрутизатору на сохранение полученных маршрутных обновлений.
protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast unsuppress-map <имя_карты_маршрутов>	Предписание локальному маршрутизатору выборочно распространять маршруты на основе маршрутной карты.
protocols bgp <номер_АС> neighbor <идентификатор> advertisement-interval <время>	Установка минимального интервала времени для обновления маршрутов.
protocols bgp <номер_АС> neighbor <идентификатор> allowas-in	Разрешение на получение объявления, содержащего атрибут AS_PATH локальному маршрутизатору.
protocols bgp <номер_АС> neighbor <идентификатор> attribute-unchanged	Разрешение локальному маршрутизатору передачи обновлений узлу с неизменными атрибутами.
protocols bgp <номер_АС> neighbor <идентификатор> capability dynamic	Объявление поддержки динамического обновления, получаемого узла.
protocols bgp <номер_АС> neighbor <идентификатор> capability orf	Объявление поддержки Outbound Route Filtering (ORF), получаемого от узла.
protocols bgp <номер_АС> neighbor <идентификатор> default-originate	Разрешение пересылки маршрута по умолчанию узлу.
protocols bgp <номер_АС> neighbor <идентификатор> description <описание>	Краткое описание узла.
protocols bgp <номер_АС> neighbor <идентификатор> disable-capability-negotiation	Отключение согласования возможностей BGP.
protocols bgp <номер_АС> neighbor <идентификатор> disable-connected-check	Отключение проверки прямого подключения для транзитного узла.
protocols bgp <номер_АС> neighbor <идентификатор> disable-send-community	Запрещение отправки расширенных атрибутов к указанному узлу.
protocols bgp <номер_АС> neighbor <идентификатор> distribute-list export <список_доступа>	Применение списка допуска, для фильтрации исходящих маршрутных обновлений к узлу.
protocols bgp <номер_АС> neighbor <идентификатор> distribute-list import <список_доступа>	Применение списка допуска, для фильтрации входящих маршрутных обновлений от узла.
protocols bgp <номер_АС> neighbor <идентификатор> ebgp-multihop <число_переходов>	Предоставление участия в динамической маршрутизации узлам, не соединенным напрямую.
protocols bgp <номер_АС> neighbor <идентификатор> filter-list export <имя_списка_путей>	Применение списка пути AS к маршрутным обновлениям до указанного узла.
protocols bgp <номер_АС> neighbor <идентификатор> filter-list import <имя_списка_путей>	Применение списка пути AS к маршрутным обновлениям от указанного узла.

protocols bgp <номер_АС> neighbor <идентификатор> local-as <номер_локальной_АС>	Определение локального номера автономной системы при пиринговой сессии.
protocols bgp <номер_АС> neighbor <идентификатор> maximum-prefix <число_префиксов>	Установка максимального числа префиксов, принимаемых узлом перед тем, как она будет переведена в нерабочее состояние.
protocols bgp <номер_АС> neighbor <идентификатор> nexthop-self	Установка локального маршрутизатора как следующего транзитного участка для узла.
protocols bgp <номер_АС> neighbor <идентификатор> override-capability	Разрешение на пиринговую сессию с узлом, который не поддерживает согласование возможностей.
protocols bgp <номер_АС> neighbor <идентификатор> passive	Предписание маршрутизатору не инициировать соединение указанным узлом.
protocols bgp <номер_АС> neighbor <идентификатор> password <пароль>	Указание хешированного в MD5 пароля.
protocols bgp <номер_АС> neighbor <идентификатор> peer-group <имя_группы>	Присваивание узла в качестве элемента группы узлов.
protocols bgp <номер_АС> neighbor <идентификатор> port <порт>	Определение порта, на котором узел прослушивает BGP-сигналы.
protocols bgp <номер_АС> neighbor <идентификатор> prefix-list export <имя_префикс-листа>	Применение префиксного списка для фильтрации обновлений к узлу.
protocols bgp <номер_АС> neighbor <идентификатор> prefix-list import <имя_префикс-листа>	Применение префиксного списка для фильтрации обновлений от узла.
protocols bgp <номер_АС> neighbor <идентификатор> remote-as <номер_АС>	Указание маршрутизатору на удаление частных АС из обновлений, отправленных на указанный узел.
protocols bgp <номер_АС> neighbor <идентификатор> remove-private-as	Предписание локальному маршрутизатору на исключение частных АС от обновлений.
protocols bgp <номер_АС> neighbor <идентификатор> route-map export <имя_карты_маршрутов>	Применение карты маршрута для фильтрации обновлений к узлу.
protocols bgp <номер_АС> neighbor <идентификатор> route-map import <имя_карты_маршрутов>	Применение карты маршрута для фильтрации обновлений от узла.
protocols bgp <номер_АС> neighbor <идентификатор> shutdown	Административное прекращение работы указанного узла.
protocols bgp <номер_АС> neighbor <идентификатор> soft-reconfiguration inbound	Предписание локальному маршрутизатору на сохранение полученных маршрутных обновлений.
protocols bgp <номер_АС> neighbor <идентификатор> strict-capability-match	Направление маршрутизатора на строгое соответствие возможностям узла.
protocols bgp <номер_АС> neighbor <идентификатор> timers	Установка таймера для узла.
protocols bgp <номер_АС> neighbor <идентификатор> ttl-security hops <число_переходов>	Установка TTL для транзитных участков для указанного узла.
protocols bgp <номер_АС> neighbor <идентификатор> unsuppress-map <имя_карты_маршрутов>	Предписание локальному маршрутизатору выборочно распространять маршруты на основе маршрутной карты.
protocols bgp <номер_АС> neighbor <идентификатор> update-source <источник>	Определение исходного IP-адреса или интерфейса маршрутных обновлений.
protocols bgp <номер_АС> neighbor <идентификатор> weight <вес>	Определение веса по умолчанию для маршрутов от указанного узла.
Операционные команды	
show ip bgp ipv4 unicast neighbors	Отображение подробной информации по однонаправленной IPv4-маршрутизации для указанного узла.
show ip bgp ipv4 unicast neighbors <идентификатор> advertised-routes	Отображение о распространении однонаправленных IPv4-маршрутов для указанного узла.

show ip bgp ipv4 unicast neighbors <идентификатор> prefix-counts	Отображение подробной информации о числе префиксов при однонаправленной IPv4-маршрутизации для указанного узла.
show ip bgp ipv4 unicast neighbors <идентификатор> received prefix-filter	Отображение подробной информации о префиксных списках при однонаправленной Ipv4-маршрутизации, полученных от указанного узла.
show ip bgp ipv4 unicast neighbors <идентификатор> received-routes	Отображение подробной информации о однонаправленных Ipv4-маршрутах, полученных от указанного узла.
show ip bgp ipv4 unicast neighbors <идентификатор> routes	Отображение подробной информации о однонаправленных Ipv4-маршрутах, полученных и принятых от указанного узла.
show ip bgp neighbors	Отображение подробной информации о узле.
show ip bgp neighbors <идентификатор> advertised-routes	Отображение информации о распространении маршрутов для указанного узла.
show ip bgp neighbors <идентификатор> dampened-routes	Отображение информации о подавленных маршрутах указанного узла.
show ip bgp neighbors <идентификатор> flap-statistics	Отображение статистики о нестабильности маршрута от указанного узла.
show ip bgp neighbors <идентификатор> prefix-counts	Отображение информации о числе префиксов для указанного узла
show ip bgp neighbors <идентификатор> received prefix-filter	Отображение подробной информации о префиксных списках от указанного узла.
show ip bgp neighbors <идентификатор> received-routes	Отображение подробной информации о маршрутах, полученных от указанного узла.
show ip bgp neighbors <идентификатор> routes	Отображение подробной информации о полученных и принятых от указанного узла.
show ipv6 bgp neighbors	Отображение подробной информации о узле.
show ipv6 bgp neighbors <идентификатор> advertised-routes	Отображение информации о распространении маршрутов для указанного узла.
show ipv6 bgp neighbors <идентификатор> received-routes	Отображение подробной информации о однонаправленных Ipv6-маршрутах, полученных от указанного узла.
show ipv6 bgp neighbors <идентификатор> routes	Отображение подробной информации о однонаправленных Ipv6-маршрутах, полученных и принятых от указанного узла.

28.4.1 protocols bgp <номер_AC> neighbor <идентификатор>

Указание узла BGP.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор>
delete protocols bgp <номер_AC> neighbor <идентификатор>
show protocols bgp <номер_AC> neighbor <идентификатор>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
      }
   }
```

```
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

идентификатор

Множественный узел. IPv4 или IPv6 адрес узла BGP. Возможно указание нескольких узлов BGP, путем создания множественных узлов конфигурации.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для указания узла BGP.

Форма **delete** этой команды используется для удаления узла BGP.

Форма **show** этой команды используется для просмотра настройки конфигурации узла BGP.

28.4.2 protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast

Определение конфигурации однонаправленных IPv6-маршрутов BGP при пиринговой сессии.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast

delete protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast

show protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            address-family {
                ipv6-unicast {
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

Множественный узел. IPv4 или IPv6 адрес узла BGP.

Значение по умолчанию

Отсутствует.

Указания по использованию

Использование этой команды определяет конфигурацию однонаправленных IPv6-маршрутов BGP при пиринговой сессии.

Форма **set** этой команды используется для указания конфигурации узлов.

Форма **delete** этой команды используется для удаления конфигурации узлов.

Форма **show** этой команды используется для просмотра настройки конфигурации узлов.

28.4.3 protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast allowas-in

Разрешение на получение объявления, содержащего атрибут AS_PATH локальному маршрутизатору.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast allowas-in [number <количество>]

delete protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast allowas-in

show protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            address-family {
                ipv6-unicast {
                    allowas-in {
                        number количество
                    }
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

идентификатор

Множественный узел. IPv4 или IPv6 адрес узла BGP.

количество

Количество попыток на получение объявления, атрибута AS_PATH локальному маршрутизатору. Диапазон составляет от 1 до 10 попыток.

Значение по умолчанию

Получение объявления атрибута AS_PATH запрещено.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для разрешения роутеру принимать объявления атрибута AS_PATH.

Форма **delete** этой команды используется для запрещения роутеру принимать объявления пути.

Форма **show** этой команды используется для просмотра настройки конфигурации.

28.4.4 protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast attribute-unchanged

Разрешение роутеру передачи обновлений узлу с неизменными атрибутами.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast attribute-unchanged [as-path | med | next-hop]

delete protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast attribute-unchanged [as-path | med | next-hop]

show protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast attribute-unchanged
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         address-family {
            ipv6-unicast {
               attribute-unchanged {
                  as-path
                  med
                  next-hop
               }
            }
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

идентификатор

Множественный узел. IPv4 или IPv6 адрес узла BGP.

as-path

Распространение обновлений маршрутов с неизменным атрибутом AS_PATH.

med

Распространение обновлений маршрутов с неизменным атрибутом Multi Exit Discriminator.

next-hop

Распространение обновлений маршрутов с неизменным атрибутом next-hop.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для разрешения передачи роутером обновлений маршрутов, без изменения атрибутов BGP: AS_PATH, MED и next-hop.

Форма **delete** этой команды используется для восстановления нормальной модификации атрибутов BGP.

Форма **show** этой команды используется для просмотра настройки конфигурации.

28.4.5 protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast capability dynamic

Объявление поддержки динамического обновления, получаемого от узла.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast capability dynamic

delete protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast capability dynamic

show protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast capability
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            address-family {
                ipv6-unicast {
                    capability {
                        dynamic
                    }
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

идентификатор

Множественный узел. IPv4 или IPv6 адрес узла BGP.

Значение по умолчанию

Пиринговая сессия функционирует с минимальными возможностями.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для объявления поддержки динамического обновления, получаемого от узла, без изменения атрибутов BGP: AS_PATH, MED и next-hop.

Форма **delete** этой команды используется для отказа возможности динамического обновления.

Форма **show** этой команды используется для просмотра настройки конфигурации.

28.4.6 protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast capability orf

Объявление поддержки Outbound Route Filtering (ORF), получаемого от узла.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast capability orf [prefix-list [receive | send]]

delete protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast capability orf

show protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            address-family {
                ipv6-unicast {
                    capability {
                        orf {
                            prefix-list {
                                receive
                                send
                            }
                        }
                    }
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

идентификатор

Множественный узел. IPv4 или IPv6 адрес узла BGP.

prefix-list

Распространение префиксного списка ORF к узлу.

receive

Возможность получения ORF от узла.

send

Возможность отправки ORF к узлу.

Значение по умолчанию

Пиринговая сессия функционирует с минимальными возможностями.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для объявления поддержки ORF.

Форма **delete** этой команды используется для отказа возможности использования ORF.

Форма **show** этой команды используется для просмотра настройки конфигурации.

28.4.7 protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast default-originate

Разрешение пересылки маршрута по умолчанию к узлу BGP.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast default-originate [route-map <имя_карты_маршрутов>]

delete protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast default-originate [route-map <имя_карты_маршрутов>]

show protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast default-originate
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            address-family {
                ipv6-unicast {
                    default-originate {
                        route-map имя_карты_маршрутов
                    }
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

идентификатор

Множественный узел. IPv4 или IPv6 адрес узла BGP.

имя_карты_маршрутов

Указание настроенной карты маршрута, которая будет использоваться при объявлении маршрута по умолчанию.

Значение по умолчанию

По умолчанию пересылка маршрута запрещена.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для разрешения локальному маршрутизатору объявлять маршрут по умолчанию ::/0 узлу. Данный маршрут используется при невозможности использования других маршрутов. Маршрут::/0 не должен быть явно сконфигурирован на локальном маршрутизаторе.

Форма **delete** этой команды используется для отключения переадресации маршрута по умолчанию или удаления карты маршрута.

Форма **show** этой команды используется для просмотра маршрута по умолчанию группы узлов.

28.4.8 protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast disable-send-community

Запрещение отправки расширенных атрибутов к указанному узлу.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast disable-send-community [extended | standard]

delete protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast disable-send-community

show protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         address-family {
            ipv6-unicast {
               disable-send-community {
                  extended
                  standard
               }
            }
         }
      }
```

```
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

идентификатор

Множественный узел. IPv4 или IPv6 адрес узла BGP.

extended

Запрещение отправки расширенных атрибутов.

standard

Запрещение отправки стандартных атрибутов.

Значение по умолчанию

Отправка атрибутов по умолчанию разрешена.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для запрещения отправки расширенных атрибутов по умолчанию.

Форма **delete** этой команды используется для восстановления настройки по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.4.9 protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast distribute-list export <список_доступа>

Применение списка доступа для фильтрации исходящих обновлений маршрутизации к узлу.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast distribute-list export <список_доступа>

delete protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast distribute-list export

show protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast distribute-list export
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            address-family {
                ipv6-unicast {
                    distribute-list {
                        export <список_доступа>
                    }
                }
            }
        }
```

```
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

идентификатор

Множественный узел. IPv4 или IPv6 адрес узла BGP.

список_доступа

Имя списка доступа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для применения списка доступа для фильтрации исходящих обновлений маршрутизации к узлу.

Форма **delete** этой команды используется для отключения распространения списка доступа для фильтрации исходящих обновлений маршрутизации к узлу.

Форма **show** этой команды используется для просмотра настройки.

28.4.10 protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast distribute-list import <список_доступа>

Применение списка доступа для фильтрации входящих обновлений маршрутизации от узла.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast distribute-list import <список_доступа>

delete protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast distribute-list import

show protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast distribute-list import
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            address-family {
                ipv6-unicast {
                    distribute-list {
                        import список_доступа
                    }
                }
            }
        }
```

```
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

список_доступа

Имя списка доступа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для применения списка доступа для фильтрации входящих обновлений маршрутизации от узла.

Форма **delete** этой команды используется для отключения распространения списка доступа для фильтрации входящих обновлений маршрутизации от узла.

Форма **show** этой команды используется для просмотра настройки.

28.4.11 protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast filter-list export <имя_списка_путей>

Применение списка пути AS к маршрутным обновлениям до указанного узла.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast filter-list export <имя_списка_путей>

delete protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast filter-list export <имя_списка_путей>

show protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         address-family {
            ipv6-unicast {
               filter-list {
                  export имя_списка_путей
               }
            }
         }
      }
   }
```

```
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

имя_списка_путей

Имя списка путей для фильтрации обновлений маршрутов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для применения списка доступа для фильтрации исходящих обновлений маршрутизации.

Форма **delete** этой команды используется для отключения исходящих обновлений маршрутизации.

Форма **show** этой команды используется для просмотра настройки.

28.4.12 protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast filter-list import <имя_списка_путей>

Применение списка пути AS к маршрутным обновлениям от указанного узла.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast filter-list import <имя_списка_путей>

delete protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast filter-list import <имя_списка_путей>

show protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast filter-list
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         address-family {
            ipv6-unicast {
               filter-list {
                  import имя_списка_путей
               }
            }
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

имя_списка_путей

Имя списка путей для фильтрации обновлений маршрутов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для применения списка доступа для фильтрации входящих обновлений маршрутизации.

Форма **delete** этой команды используется для отключения входящих обновлений маршрутизации.

Форма **show** этой команды используется для просмотра настройки.

28.4.13 protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast maximum-prefix <число_префиксов>

Установка максимального числа префиксов, принимаемых узлом перед тем как он будет переведена в нерабочее состояние.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast maximum-prefix <число_префиксов>

delete protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast maximum-prefix <число_префиксов>

show protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp <номер_AC> {
       neighbor <идентификатор>{
           address-family {
                  ipv6-unicast {
                        maximum-prefix <число_префиксов>
                        }
                 }
              }
       }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой АС для использования в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для приватных АС, использующихся

локально.

идентификатор

IPv4- или IPv6-адрес BGP-соседа. Возможно указание нескольких соседей, путем создания нескольких узлов конфигурации.

число_префиксов

Максимальное число префиксов, принимаемых узлом перед тем как он будет переведена в нерабочее состояние.

Значение по умолчанию

Максимальное число префиксов не указывается.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для установки максимального числа префиксов.

Форма **delete** этой команды используется для удаления настройки.

Форма **show** этой команды используется для просмотра настройки.

28.4.14 protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast nexthop-local unchanged

Указание IPv6-адреса, не изменяемого при анонсировании префикса узлом.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор>  address-family ipv6-unicast nexthop-local unchanged

delete protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast nexthop-local

show protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast nexthop-local
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         address-family {
            ipv6-unicast {
               nexthop-local {
                  unchanged
               }
            }
         }
      }
   }
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

Значение по умолчанию

IPv6-адрес не меняется при анонсировании префикса узлом.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для указания IPv6-адреса, не изменяемого при анонсировании префикса узлом.

Форма **delete** этой команды используется для восстановления настроек по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.4.15 protocols bgp <номер_АС> neighbor <идентификатор> address-family ipv6-unicast nexthop-self

Установка локального маршрутизатора как следующего транзитного участка для узла.

Синтаксис

```
set protocols bgp <номер_АС> neighbor <идентификатор>  address-family ipv6-unicast nexthop-self

delete protocols bgp <номер_АС> neighbor <идентификатор>  address-family ipv6-unicast nexthop-self

show protocols bgp <номер_АС> neighbor <идентификатор>  address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_АС {
        neighbor идентификатор {
            address-family {
                ipv6-unicast {
                    nexthop-self
                }
            }
        }
    }
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

Значение по умолчанию

Запрещено.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для установки локального маршрутизатора как следующего транзитного участка для узла.

Форма **delete** этой команды используется для удаления настройки.

Форма **show** этой команды используется для просмотра настройки.

28.4.16 protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast prefix-list export <имя_префикс-листа>

Применение префиксного списка для фильтрации обновлений к узлу.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор>  address-family ipv6-unicast prefix-list export <имя_префикс-листа>

delete protocols bgp <номер_AC> neighbor <идентификатор>  address-family ipv6-unicast prefix-list export <имя_префикс-листа>

show protocols bgp <номер_AC> neighbor <идентификатор>  address-family ipv6-unicast prefix-list
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         address-family {
            ipv6-unicast {
               prefix-list {
                  export имя_префикс-листа
               }
            }
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

имя_префикс-листа

Название сконфигурированного префиксного списка.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для ограничения распространения исходящей информации о узле используя фильтрование с помощью префиксного списка.

Форма **delete** этой команды используется для удаления префиксного фильтра.

Форма **show** этой команды используется для просмотра настройки.

28.4.17 protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast prefix-list import <имя_префикс-листа>

Применение префиксного списка для фильтрации обновлений от узла.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast prefix-list import <имя_префикс-листа>

delete protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast prefix-list import <имя_префикс-листа>

show protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast prefix-list
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            address-family {
                ipv6-unicast {
                    prefix-list {
                        import имя_префикс-листа
                    }
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

имя_префикс-листа

Название сконфигурированного префиксного списка.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для ограничения распространения входящей информации о узле используя фильтрование с помощью префиксного списка.

Форма **delete** этой команды используется для удаления префиксного фильтра.

Форма **show** этой команды используется для просмотра настройки.

28.4.18 protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast remove-private-as

Предписание локальному маршрутизатору на исключение частных AC от обновлений.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast remove-private-as

delete protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast remove-private-as

show protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор
{          address-family {
             ipv6-unicast {
                remove-private-as
             }
          }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

Значение по умолчанию

Частные AC включены в исходящие обновления.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для указания локальному маршрутизатору об исключении частных AC от обновлений. При активации данной функции, маршрутизатор отпускает частные AC от атрибута AS_PATH. Команда может использоваться в конфедерациях при условии, что частные AS добавлены после части конфедерации пути AS. Данная команда применяется только к узлам eBGP; и не может использоваться с узлами iBGP.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.4.19 protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast route-map export <имя_карты_маршрутов>

Применение карты маршрута для фильтрации обновлений к узлу.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast route-map export <имя_карты_маршрутов>

delete protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast route-map export <имя_карты_маршрутов>

show protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast route-map export
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            address-family {
                ipv6-unicast {
                    route-map {
                        export имя_карты_маршрутов
                    }
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

имя_карты_маршрутов

Указание настроенной карты маршрута, которая будет использоваться при объявлении маршрута по умолчанию.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для ограничения распределение исходящей информации о узле используя фильтрацию карты маршрута.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.4.20 protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast route-map import <имя_карты_маршрутов>

Применение карты маршрута для фильтрации обновлений от узла.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast route-map import <имя_карты_маршрутов>

delete protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast route-map import <имя_карты_маршрутов>

show protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast route-map import
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            address-family {
                ipv6-unicast {
                    route-map {
                        import имя_карты_маршрутов
                    }
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

имя_карты_маршрутов

Указание настроенной карты маршрута, которая будет использоваться при объявлении маршрута по умолчанию.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для ограничения распределение входящей информации об узле используя фильтрацию карты маршрута.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.4.21 protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast soft-reconfiguration inbound

Предписание локальному маршрутизатору на сохранение полученных маршрутных обновлений.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast soft-reconfiguration inbound

delete protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast soft-reconfiguration inbound

show protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            address-family {
                ipv6-unicast {
                    soft-reconfiguration {
                        inbound
                    }
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для включения режима мягкого реконфигурирования, при котором локальный маршрутизатор сохраняет маршрутные обновления.

Форма **delete** этой команды используется для отключения мягкого реконфигурирования.

Форма **show** этой команды используется для просмотра настройки.

28.4.22 protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast unsuppress-map <имя_карты_маршрутов>

Предписание локальному маршрутизатору выборочно распространять маршруты на основе маршрутной карты.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast unsuppress-map <имя_карты_маршрутов>

delete protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast unsuppress-map <имя_карты_маршрутов>

show protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         address-family {
            ipv6-unicast {
               unsuppress-map имя_карты_маршрутов
            }
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

идентификатор

IPv4- или IPv6-адрес BGP-соседа. Возможно указание нескольких соседей, путем создания нескольких узлов конфигурации.

имя_карты_маршрутов

Указание настроенной карты маршрута, которая будет использоваться при объявлении маршрута по умолчанию.

Значение по умолчанию

Маршруты не распространяются.

Указания по использованию

Эта команда применяется только при однонаправленной IPv6-маршрутизации.

Форма **set** этой команды используется для выборочного распространения маршрутов.

Форма **delete** этой команды используется для восстановления настроек по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.4.23 protocols bgp <номер_AC> neighbor <идентификатор> advertisement-interval <время>

Установка минимального интервала времени для обновления маршрутов.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> advertisement-interval <время>
```

```
delete protocols bgp <номер_AC> neighbor <идентификатор> advertisement-interval
```

```
show protocols bgp <номер_AC> neighbor <идентификатор>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            advertisement-interval <время>
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

время

Минимальный интервал времени, в секундах, между обновлением маршрута указанного узла. Диапазон составляет от 0 до 600 секунд.

Значение по умолчанию

По умолчанию интервал составляет 30 секунд для eBGP-узлов, и 5 секунд для iBGP-узлов.

Указания по использованию

Форма **set** этой команды используется для установки минимального интервала времени для обновления маршрутов.

Форма **delete** этой команды используется для восстановления настроек по умолчанию.

Форма **show** этой команды используется для просмотра настройки конфигурации.

28.4.24 protocols bgp <номер_AC> neighbor <идентификатор> allowas-in

Разрешение на получение объявления, содержащего атрибут AS_PATH локальному маршрутизатору.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> allowas-in [number <количество>]
```

```
delete protocols bgp <номер_AC> neighbor <идентификатор> allowas-in
```

```
show protocols bgp <номер_AC> neighbor <идентификатор>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            allowas-in {
```

```
                number количество
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

количество

Количество попыток на получение объявления, атрибута AS_PATH локальному маршрутизатору. Диапазон составляет от 1 до 10 попыток. По умолчанию установлено 3 попытки.

Значение по умолчанию

Получение объявления атрибута AS_PATH запрещено.

Указания по использованию

Форма **set** этой команды используется для разрешения локальному маршрутизатору принимать объявления атрибута AS_PATH.

Форма **delete** этой команды используется для запрещения локальному маршрутизатору принимать объявления атрибута AS_PATH.

Форма **show** этой команды используется для просмотра настройки конфигурации.

28.4.25 protocols bgp <номер_AC> neighbor <идентификатор> attribute-unchanged

Разрешение локальному маршрутизатору передачи обновлений узлу с неизменными атрибутами.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> attribute-unchanged [as-path | med | next-hop]

delete protocols bgp <номер_AC> neighbor <идентификатор> attribute-unchanged [as-path | med | next-hop]

show protocols bgp <номер_AC> neighbor <идентификатор> attribute-unchanged
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            attribute-unchanged {
                as-path
                med
                next-hop
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

as-path

Распространяет маршрутное обновление с неизменным атрибутом AS_PATH.

med

Маршрутное обновление с неизменным атрибутом AS_PATH.

next-hop

Маршрутное обновление с неизменным атрибутом next-hop.

Значение по умолчанию

Запрещено.

Указания по использованию

Форма **set** этой команды используется для разрешения передачи локальным маршрутизатором обновлений маршрутов, без изменения атрибутов BGP: AS_PATH, MED и next-hop.

Форма **delete** этой команды используется для восстановления нормальной модификации атрибутов BGP.

Форма **show** этой команды используется для просмотра настройки конфигурации.

28.4.26 protocols bgp <номер_AC> neighbor <идентификатор> capability dynamic

Объявление поддержки динамического обновления, получаемого от узла.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> capability dynamic
delete protocols bgp <номер_AC> neighbor <идентификатор> capability dynamic
show protocols bgp <номер_AC> neighbor <идентификатор> capability
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {          capability {
            dynamic
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

Значение по умолчанию

Пиринговая сессия функционирует с минимальными возможностями.

Указания по использованию

Форма **set** этой команды используется для объявления поддержки динамического обновления.

Форма **delete** этой команды используется для отказа возможности динамического обновления.

Форма **show** этой команды используется для просмотра настройки конфигурации.

28.4.27 protocols bgp <номер_AC> neighbor <идентификатор> capability orf

Объявление поддержки Outbound Route Filtering (ORF), получаемого от узла.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> capability orf [prefix-list [receive | send]]

delete protocols bgp <номер_AC> neighbor <идентификатор> capability orf

show protocols bgp <номер_AC> neighbor <идентификатор> capability orf
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            capability {
                orf {
                    prefix-list {
                        receive
                        send
                    }
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

receive

Возможность получения ORF от узла.

send

Возможность отправки ORF к узлу.

Значение по умолчанию

Пиринговая сессия функционирует с минимальными возможностями.

Указания по использованию

Форма **set** этой команды используется для объявления поддержки ORF.

Форма **delete** этой команды используется для отказа возможности использования ORF.

Форма **show** этой команды используется для просмотра настройки конфигурации.

28.4.28 protocols bgp <номер_AC> neighbor <идентификатор> default-originate

Разрешение пересылки маршрута по умолчанию узлу.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> default-originate [route-map <имя_карты_маршрутов>]

delete protocols bgp <номер_AC> neighbor <идентификатор> default-originate [route-map <имя_карты_маршрутов>]

show protocols bgp <номер_AC> neighbor <идентификатор> default-originate
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         default-originate {
            route-map имя_карты_маршрутов
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

имя_карты_маршрутов

Указание настроенной карты маршрута, которая будет использоваться при объявлении маршрута по умолчанию.

Значение по умолчанию

По умолчанию пересылка маршрута запрещена.

Указания по использованию

Форма **set** этой команды используется для разрешения локальному маршрутизатору объявлять маршрут по умолчанию ::/0 узлу. Данный маршрут используется при невозможности использования других маршрутов. Маршрут::/0 не должен быть явно сконфигурирован на локальном маршрутизаторе.

Форма **delete** этой команды используется для отключения переадресации маршрута по умолчанию или удаления карты маршрута.

Форма **show** этой команды используется для просмотра маршрута по умолчанию группы узлов.

28.4.29 protocols bgp <номер_AC> neighbor <идентификатор> description <описание>

Краткое описание узла.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> description <описание>
delete protocols bgp <номер_AC> neighbor <идентификатор> description
show protocols bgp <номер_AC> neighbor <идентификатор>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         description <описание>
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

описание

Описание узла.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для краткого описания узла.

Форма **delete** этой команды используется для удаления краткого описания группы узла.

Форма **show** этой команды используется для просмотра настройки.

28.4.30 protocols bgp <номер_AC> neighbor <идентификатор> disable-capability-negotiation

Отключение согласования возможностей BGP.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> disable-capability-negotiation
delete protocols bgp <номер_AC> neighbor <идентификатор> disable-capability-negotiation
show protocols bgp <номер_AC> neighbor <идентификатор>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         disable-capability-negotiation
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

Значение по умолчанию

Согласования возможностей BGP выполняется.

Указания по использованию

Форма **set** этой команды используется для отключения согласования возможностей BGP.

Форма **delete** этой команды используется для удаления этого атрибута и восстановления согласования возможностей BGP.

Форма **show** этой команды используется для просмотра настройки.

28.4.31 protocols bgp <номер_AC> neighbor <идентификатор> disable-connected-check

Отключение проверки прямого подключения для транзитного узла.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> disable-connected-check
delete protocols bgp <номер_AC> neighbor <идентификатор> disable-connected-check
show protocols bgp <номер_AC> neighbor <идентификатор>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         disable-connected-check
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

Значение по умолчанию

Проверка соединения выполняется.

Указания по использованию

Форма **set** этой команды используется для отключения проверки соединения для транзитного узла.

Форма **delete** этой команды используется для восстановления проверки соединения для транзитного узла.

Форма **show** этой команды используется для просмотра настройки.

28.4.32 protocols bgp <номер_AC> neighbor <идентификатор> disable-send-community

Запрещение отправки расширенных атрибутов к указанному узлу.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> disable-send-community [extended | standard]

delete protocols bgp <номер_AC> neighbor <идентификатор> disable-send-community

show protocols bgp <номер_AC> neighbor <идентификатор>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         disable-send-community {
            extended
            standard
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

идентификатор

IPv4- или IPv6-адрес BGP-соседа. Возможно указание нескольких соседей, путем создания нескольких узлов конфигурации.

extended

Запрещение отправки расширенных атрибутов.

standard

Запрещение отправки стандартных атрибутов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для настройки запрещает отправку расширенных атрибутов по умолчанию.

Форма **delete** этой команды используется для восстановления настройки по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.4.33 protocols bgp <номер_AC> neighbor <идентификатор> distribute-list export <список_доступа>

Применение списка допуска, для фильтрации исходящих маршрутных обновлений к узлу.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> distribute-list export <список_доступа>

delete protocols bgp <номер_AC> neighbor <идентификатор> distribute-list <список_доступа>

show protocols bgp <номер_AC> neighbor <идентификатор> distribute-list
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            distribute-list {
                export список_доступа
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

список_доступа

Число стандартного или расширенного списка доступа. Диапазон для стандартного списка доступа равняется 1 - 99. Диапазон для расширенного списка доступа равняется 100 - 199.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для применения списка допуска, для фильтрации исходящих маршрутных обновлений к узлу.

Форма **delete** этой команды используется для восстановления настройки по умолчанию.

Форма **show** этой команды используется для просмотра настройки конфигурации BGP соседа.

28.4.34 protocols bgp <номер_AC> neighbor <идентификатор> distribute-list import <список_доступа>

Применение списка допуска, для фильтрации входящих маршрутных обновлений от узла.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> distribute-list import <список_доступа>

delete protocols bgp <номер_AC> neighbor <идентификатор> distribute-list <список_доступа>

show protocols bgp <номер_AC> neighbor <идентификатор> distribute-list
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            distribute-list {
                import список_доступа
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

список_доступа

Число стандартного или расширенного списка доступа. Диапазон для стандартного списка доступа равняется 1 - 99. Диапазон для расширенного списка доступа равняется 100 - 199.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для применения списка допуска, для фильтрации входящих маршрутных обновлений от узла.

Форма **delete** этой команды используется для восстановления настройки по умолчанию.

Форма **show** этой команды используется для просмотра настройки конфигурации BGP соседа.

28.4.35 protocols bgp <номер_AC> neighbor <идентификатор> ebgp-multihop <число_переходов>

Предоставление участия в динамической маршрутизации узлам, не соединенным напрямую.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> ebgp-multihop <число_переходов>

delete protocols bgp <номер_AC> neighbor <идентификатор> ebgp-multihop
```

```
show protocols bgp  <номер_AC> neighbor <идентификатор>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         ebgp-multihop <число_переходов>
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

число_переходов

Время жизни или максимальное количество возможных транзитных участков. Диапазон 1 — 255.

Значение по умолчанию

Участие в динамической маршрутизации возможно только узлам соединенным напрямую.

Указания по использованию

Форма **set** этой команды используется для предоставления участия в динамической маршрутизации узлам, не соединенным напрямую.

Форма **delete** этой команды используется для восстановления настройки по умолчанию.

Форма **show** этой команды используется для просмотра настройки конфигурации BGP соседа.

28.4.36 protocols bgp <номер_AC> neighbor <идентификатор> filter-list export <имя_списка_путей>

Применение списка пути AS к маршрутным обновлениям до указанного узла.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> filter-list export
<имя_списка_путей>

delete protocols bgp <номер_AC> neighbor <идентификатор> filter-list export
<имя_списка_путей>

show protocols bgp <номер_AC> neighbor <идентификатор> filter-list
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         filter-list {
            export имя_списка_путей
```

```
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

имя_списка_путей

Наименование автономной системы.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для применения списка доступа для фильтрации исходящих обновлений маршрутизации.

Форма **delete** этой команды используется для отключения исходящих обновлений маршрутизации.

Форма **show** этой команды используется для просмотра настройки.

28.4.37 protocols bgp <номер_AC> neighbor <идентификатор> filter-list import <имя_списка_путей>

Применение списка пути AS к маршрутным обновлениям от указанного узла.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> filter-list import <имя_списка_путей>
delete protocols bgp <номер_AC> neighbor <идентификатор> filter-list import <имя_списка_путей>
show protocols bgp <номер_AC> neighbor <идентификатор> filter-list
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {          filter-list {
                import имя_списка_путей
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

имя_списка_путей

Наименование автономной системы.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для применения списка доступа для фильтрации входящих обновлений маршрутизации.

Форма **delete** этой команды используется для отключения входящих обновлений маршрутизации.

Форма **show** этой команды используется для просмотра настройки.

28.4.38 protocols bgp <номер_AC> neighbor <идентификатор> local-as <номер_локальной_AC>

Определение локального номера автономной системы при пиринговой сессии.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> local-as <номер_локальной_AC> [no-prepend]

delete protocols bgp <номер_AC> neighbor <идентификатор> local-as <номер_локальной_AC> [no-prepend]

show protocols bgp <номер_AC> neighbor <идентификатор>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         local-as номер_локальной_AC {
            no-prepend
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

номер_локальной_AC

Допустимый номер AC. Нельзя использовать число AC, которому принадлежит группа узлов. Значение должно лежать в диапазоне от 1 до 4294967294.

no-prepend

Указание маршрутизатору не ожидать номер локальный AC к маршрутам, полученным от внешнего узла.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для указания номер локальной АС при пиринговой сессии.

Форма **delete** этой команды используется для удаления номер локальной АС.

Форма **show** этой команды используется для просмотра настройки.

28.4.39 protocols bgp <номер_АС> neighbor <идентификатор> maximum-prefix <число_префиксов>

Установка максимального числа префиксов, принимаемых узлом перед тем как он будет переведен в нерабочее состояние.

Синтаксис

```
set protocols bgp <номер_АС> neighbor <идентификатор> maximum-prefix <число_префиксов>

delete protocols bgp <номер_АС> neighbor <идентификатор> maximum-prefix <число_префиксов>

show protocols bgp <номер_АС> neighbor <идентификатор> maximum-prefix
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_АС {
      neighbor идентификатор {
         maximum-prefix число_префиксов
      }
   }
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

число_префиксов

Максимальное число префиксов, принимаемых узлом перед тем как он будет переведен в нерабочее состояние.

Значение по умолчанию

Максимальное число префиксов не указывается.

Указания по использованию

Форма **set** этой команды используется для установки максимального числа префиксов.

Форма **delete** этой команды используется для удаления настройки.

Форма **show** этой команды используется для просмотра настройки.

28.4.40 protocols bgp <номер_АС> neighbor <идентификатор> nexthop-self

Установка локального маршрутизатора как следующего транзитного участка для узла.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> nexthop-self
delete protocols bgp <номер_AC> neighbor <идентификатор> nexthop-self
show protocols bgp <номер_AC>  neighbor <идентификатор>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         nexthop-self
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

Значение по умолчанию

Запрещено.

Указания по использованию

Форма **set** этой команды используется для установки локального маршрутизатора как следующего транзитного участка для узла.

Форма **delete** этой команды используется для удаления настройки.

Форма **show** этой команды используется для просмотра настройки.

28.4.41 protocols bgp <номер_AC> neighbor <идентификатор> override-capability

Разрешение на пиринговую сессию с узлом, который не поддерживает согласование возможностей.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> override-capability
delete protocols bgp <номер_AC> neighbor <идентификатор> override-capability
show protocols bgp <номер_AC> neighbor <идентификатор>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         override-capability
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

Значение по умолчанию

Пиринговая сессия не может быть установлена, если узел не поддерживает согласование возможностей.

Указания по использованию

Форма **set** этой команды используется для для разрешения пиринговой сессии с узлом, который не поддерживает согласование возможностей. Как правило, если узел не поддерживает согласование возможностей, пиринговая сессия не может быть установлена.

Форма **delete** этой команды используется для восстановления настройки по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.4.42 protocols bgp <номер_AC> neighbor <идентификатор> passive

Предписание маршрутизатору не инициировать соединение указанным узлом.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> passive
delete protocols bgp <номер_AC> neighbor <идентификатор> passive
show protocols bgp <номер_AC> neighbor <идентификатор>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         passive
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

идентификатор

IPv4- или IPv6-адрес BGP-соседа. Возможно указание нескольких соседей, путем создания нескольких узлов конфигурации.

Значение по умолчанию

Маршрутизатор принимает входящие соединения и инициирует исходящие соединения.

Указания по использованию

Форма **set** этой команды используется для настройки маршрутизатора таким образом, чтобы осуществлялся прием входящих сообщений от узла, но в то же время не происходило инициализации исходящих сообщений.

Форма **delete** этой команды используется для восстановления настройки по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.4.43 protocols bgp <номер_AC> neighbor <идентификатор> password <пароль>

Указание хешированного в MD5 пароля.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> password <пароль>
delete protocols bgp <номер_AC> neighbor <идентификатор> password <пароль>
show protocols bgp <номер_AC>  neighbor <идентификатор> password
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         password пароль
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

пароль

Пароль, хешированный в MD5.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для указания хешированного в MD5 пароля.

Форма **delete** этой команды используется для удаления настройки.

Форма **show** этой команды используется для просмотра настройки конфигурации BGP соседа.

28.4.44 protocols bgp <номер_AC> neighbor <идентификатор> peer-group <имя_группы>

Присваивание узла в качестве элемента группы узлов.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> peer-group <имя_группы>
delete protocols bgp <номер_AC> neighbor <идентификатор> peer-group <имя_группы>
show protocols bgp <номер_AC> neighbor <идентификатор> peer-group
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         peer-group имя_группы
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

имя_группы

Многоузловой. Название группы узлов.

Значение по умолчанию

По умолчанию элементы группы узлов наследуют все сконфигурированные параметры настройки группы узлов.

Указания по использованию

Форма **set** этой команды используется для присваивания узла в качестве элемента группы узлов.

Форма **delete** этой команды используется для удаления узла из группы узлов.

Форма **show** этой команды используется для просмотра настройки конфигурации.

28.4.45 protocols bgp <номер_AC> neighbor <идентификатор> port <порт>

Определение порта, на котором узел прослушивает BGP-сигналы.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> port <порт>
delete protocols bgp <номер_AC> neighbor <идентификатор> port
show protocols bgp <номер_AC> neighbor <идентификатор> port
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         port порт
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

порт

Порт, на котором узел прослушивает BGP-сигналы. Диапазон 1 - 65535. Значение по умолчанию равняется 179.

Значение по умолчанию

Порт по умолчанию - 179.

Указания по использованию

Форма **set** этой команды используется для определения порта, на котором узел прослушивает BGP-сигналы.

Форма **delete** этой команды используется для восстановления порта по умолчанию.

Форма **show** этой команды используется для просмотра настройки конфигурации.

28.4.46 protocols bgp <номер_AC> neighbor <идентификатор> prefix-list export <имя_префикс-листа>

Применение префиксного списка для фильтрации обновлений к узлу.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> prefix-list export <имя_префикс-листа>
delete protocols bgp <номер_AC> neighbor <идентификатор> prefix-list export <имя_префикс-листа>
show protocols bgp <номер_AC> neighbor <идентификатор> prefix-list
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            prefix-list {
                export имя_префикс-листа
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

имя_префикс-листа

Название сконфигурированного префиксного списка.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для ограничения распространения исходящей информации о узле используя фильтрование с помощью префиксного списка.

Форма **delete** этой команды используется для удаления префиксного фильтра.

Форма **show** этой команды используется для просмотра настройки.

28.4.47 protocols bgp <номер_AC> neighbor <идентификатор> prefix-list import <имя_префикс-листа>

Применение префиксного списка для фильтрации обновлений от узла.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> prefix-list import <имя_префикс-листа>

delete protocols bgp <номер_AC> neighbor <идентификатор> prefix-list import <имя_префикс-листа>

show protocols bgp <номер_AC> neighbor <идентификатор> prefix-list
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            prefix-list {
                import имя_префикс-листа
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

имя_префикс-листа

Название сконфигурированного префиксного списка.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для ограничения распространения входящей информации о узле используя фильтрование с помощью префиксного списка.

Форма **delete** этой команды используется для удаления префиксного фильтра.

Форма **show** этой команды используется для просмотра настройки.

28.4.48 protocols bgp <номер_AC> neighbor <идентификатор> remote-as <номер_AC>

Указание маршрутизатору на удаление частных AC из обновлений, отправленных на указанный узел.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> remote-as <номер_AC>
delete protocols bgp <номер_AC> neighbor <идентификатор> remote-as
show protocols bgp <номер_AC>  neighbor <идентификатор> remote-as
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         remote-as номер_AC
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

Значение по умолчанию

Частные AC включены в исходящие обновления.

Указания по использованию

Эта команда применяется только к коллегам eBGP; это не может использоваться с коллегами iBGP.

Форма **set** этой команды используется для указания маршрутизатору на удаление частных AC из обновлений, отправленных на указанный узел. При активации данной опции, маршрутизатор при обновлении пропускает частные AC. Диапазон номеров для частных AC варьируется от 64512 до 65534.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.4.49 protocols bgp <номер_AC> neighbor <идентификатор> remove-private-as

Предписание локальному маршрутизатору на исключение частных AC от обновлений.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> remove-private-as
delete protocols bgp <номер_AC> neighbor <идентификатор> remove-private-as
show protocols bgp <номер_AC> neighbor <идентификатор>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         remove-private-as
      }
```

```
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

Значение по умолчанию

Частные AC включены в исходящие обновления.

Указания по использованию

Форма **set** этой команды используется для указания локальному маршрутизатору об исключении частных AC от обновлений. При активации данной функции, маршрутизатор отпускает частные AC от атрибута AS_PATH. Команда может использоваться в конфедерациях при условии, что частные AS добавлены после части конфедерации пути AS. Данная команда применяется только к узлам eBGP; и не может использоваться с узлами iBGP.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.4.50 protocols bgp <номер_AC> neighbor <идентификатор> route-map export <имя_карты_маршрутов>

Применение карты маршрута для фильтрации обновлений к указанному узлу.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> route-map export <имя_карты_маршрутов>

delete protocols bgp <номер_AC> neighbor <идентификатор> route-map export <имя_карты_маршрутов>

show protocols bgp <номер_AC> neighbor <идентификатор> route-map export <имя_карты_маршрутов>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            route-map {
                export имя_карты_маршрутов
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

имя_карты_маршрутов

Указание настроенной карты маршрута, которая будет использоваться при объявлении маршрута по умолчанию.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для ограничения распределение исходящей информации о узле используя фильтрацию карты маршрута.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.4.51 protocols bgp <номер_AC> neighbor <идентификатор> route-map import <имя_карты_маршрутов>

Применение карты маршрута для фильтрации обновлений от указанного узла.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> route-map import <имя_карты_маршрутов>

delete protocols bgp <номер_AC> neighbor <идентификатор> route-map import <имя_карты_маршрутов>

show protocols bgp <номер_AC> neighbor <идентификатор> route-map import <имя_карты_маршрутов>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            route-map {
                import имя_карты_маршрутов
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

имя_карты_маршрутов

Указание настроенной карты маршрута, которая будет использоваться при объявлении маршрута по умолчанию.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для ограничения распределение входящей информации о узле используя фильтрацию карты маршрута.

Форма **delete** этой команды используется для восстановления значения по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.4.52 protocols bgp <номер_AC> neighbor <идентификатор> shutdown

Административное прекращение работы указанного узла.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> shutdown
delete protocols bgp <номер_AC> neighbor <идентификатор> shutdown
show protocols bgp <номер_AC> neighbor <идентификатор>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         shutdown
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

идентификатор

IPv4- или IPv6-адрес BGP-соседа. Возможно указание нескольких соседей, путем создания нескольких узлов конфигурации.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для административного прекращения работы указанного узла. Прекращение работы маршрутизатора завершает любые активные сеансы указанного узла и удаляет любую связанную маршрутную информацию.

Форма **delete** этой команды используется для повторного начала работы указанного узла.

Форма **show** этой команды используется для просмотра настройки.

28.4.53 protocols bgp <номер_AC> neighbor <идентификатор> soft-reconfiguration inbound

Предписание локальному маршрутизатору на сохранение полученных маршрутных обновлений.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> soft-reconfiguration inbound

delete protocols bgp <номер_AC> neighbor <идентификатор> soft-reconfiguration inbound

show protocols bgp <номер_AC> neighbor <идентификатор>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         soft-reconfiguration {
            inbound
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для включения режима мягкого реконфигурирования, при котором локальный маршрутизатор сохраняет маршрутные обновления.

Форма **delete** этой команды используется для отключения мягкого реконфигурирования.

Форма **show** этой команды используется для просмотра настройки.

28.4.54 protocols bgp <номер_AC> neighbor <идентификатор> strict-capability-match

Направление маршрутизатора на строгое соответствие возможностям узла.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> strict-capability-match

delete protocols bgp <номер_AC> neighbor <идентификатор> strict-capability-match

show protocols bgp <номер_AC> neighbor <идентификатор>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
```

```
            strict-capability-match
        }
    }
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

Значение по умолчанию

Запрещено.

Указания по использованию

Форма **set** этой команды используется для направления маршрутизатору на строгое соответствие возможностям узла.

Форма **delete** этой команды используется для отключения строгого соответствия возможностям узла.

Форма **show** этой команды используется для просмотра настройки.

28.4.55 protocols bgp <номер_АС> neighbor <идентификатор> timers

Установка таймера для узла.

Синтаксис

```
set protocols bgp <номер_АС> neighbor <идентификатор> timers [connect <время> | keepalive <время> | holdtime <время>]

delete protocols bgp <номер_АС> neighbor <идентификатор> timers [connect | keepalive | holdtime]

show protocols bgp <номер_АС> neighbor <идентификатор> timers
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_АС {
        neighbor идентификатор {
            timers {
                connect время
                keepalive время
                holdtime время
            }
        }
    }
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

connect *время*

Таймаут соединения для данного соседа

keepalive *время*

Интервал удержания для данного соседа

holdtime *время*

Интервал keepalive для данного соседа

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для узла.

Форма **delete** этой команды используется для отключения строгого соответствия возможностям узла.

Форма **show** этой команды используется для просмотра настройки.

28.4.56 protocols bgp <номер_AC> neighbor <идентификатор> ttl-security hops <число_переходов>

Установка TTL для транзитных участков для указанного узла.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> ttl-security hops <число_переходов>
delete protocols bgp <номер_AC> neighbor <идентификатор> ttl-security <число_переходов>
show protocols bgp <номер_AC> neighbor <идентификатор> ttl-security hops
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            ttl-security {
                hops число_переходов
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

Обязательный. IPv4- или IPv6-адрес BGP-соседа.

число_переходов

Максимальное количество принятых на время пиринговой сессии транзитных участков от локальной узла. Значение должно лежать в диапазоне от 1 до 254.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для определения числа транзитных участков.

Форма **delete** этой команды используется для восстановления настроек по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.4.57 protocols bgp <номер_AC> neighbor <идентификатор> unsuppress-map <имя_карты_маршрутов>

Предписание локальному маршрутизатору выборочно распространять маршруты на основе маршрутной карты.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> unsuppress-map <имя_карты_маршрутов>

delete protocols bgp <номер_AC> neighbor <идентификатор> unsuppress-map <имя_карты_маршрутов>

show protocols bgp <номер_AC> neighbor <идентификатор> unsuppress-map
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         unsuppress-map имя_карты_маршрутов
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

имя_карты_маршрутов

Указание настроенной карты маршрута, которая будет использоваться при объявлении маршрута по умолчанию.

Значение по умолчанию

Маршруты не распространяются.

Указания по использованию

Форма **set** этой команды используется для выборочного распространения маршрутов.

Форма **delete** этой команды используется для восстановления настроек по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.4.58 protocols bgp <номер_AC> neighbor <идентификатор> update-source <источник>

Определение исходного IP-адреса или интерфейса маршрутных обновлений.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> update-source <источник>
delete protocols bgp <номер_AC> neighbor <идентификатор> update-source
show protocols bgp <номер_AC> neighbor <идентификатор> update-source
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      neighbor идентификатор {
         update-source источник
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

источник

IPv4-адрес маршрутизатора или интерфейса откуда поступают маршрутные обновления.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для настройки системы получать маршрутные обновления из определенного источника.

Форма **delete** этой команды используется для удаления настройки.

Форма **show** этой команды используется для просмотра настройки.

28.4.59 protocols bgp <номер_AC> neighbor <идентификатор> weight <вес>

Определение веса по умолчанию для маршрутов от указанного узла.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> weight <вес>
delete protocols bgp <номер_AC> neighbor <идентификатор> weight
show protocols bgp <номер_AC> neighbor <идентификатор> weight
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
```

```
    bgp номер_AC {
        neighbor идентификатор {
            weight вес
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC для использования в BGP маршрутизации.

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

вес

Вес который присваивается маршрутам от указанного узла. Значение должно лежать в диапазоне от 0 до 65535.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для установки значения весов маршрутов.

Форма **delete** этой команды используется для восстановления настроек по умолчанию.

Форма **show** этой команды используется для просмотра настройки.

28.4.60 show ip bgp ipv4 unicast neighbors

Отображение подробной информации по однонаправленной IPv4-маршрутизации для указанного узла.

Синтаксис

```
show ip bgp ipv4 unicast neighbors [<идентификатор>]
```

Режим ввода команды

Эксплуатационный режим.

Параметры

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

Значение по умолчанию

Информация о однонаправленной IPv4-маршрутизации показана для всех узлов.

Указания по использованию

Эта команда используется для отображения подробной информации по однонаправленной IPv4-маршрутизации для указанного узла.

28.4.61 show ip bgp ipv4 unicast neighbors <идентификатор> advertised-routes

Отображение о распространении однонаправленных IPv4-маршрутов для указанного узла.

Синтаксис

```
show ip bgp ipv4 unicast neighbors <идентификатор> advertised-routes
```

Режим ввода команды

Эксплуатационный режим.

Параметры

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения о распространении однонаправленных IPv4-маршрутов для указанного узла.

28.4.62 show ip bgp ipv4 unicast neighbors <идентификатор> prefix-counts

Отображение подробной информации о числе префиксов при однонаправленной IPv4-маршрутизации для указанного узла.

Синтаксис

```
show ip bgp ipv4 unicast neighbors <идентификатор> prefix-counts
```

Режим ввода команды

Эксплуатационный режим.

Параметры

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения подробной информации о числе префиксов при однонаправленной IPv4-маршрутизации для указанного узла.

28.4.63 show ip bgp ipv4 unicast neighbors <идентификатор> received prefix-filter

Отображение подробной информации о префиксных списках при однонаправленной IPv4-маршрутизации полученных от указанного узла.

Синтаксис

```
show ip bgp ipv4 unicast neighbors <идентификатор> received prefix-filter
```

Режим ввода команды

Эксплуатационный режим.

Параметры

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения подробной информации о префиксных списках при однонаправленной IPv4-маршрутизации полученных от указанного узла.

28.4.64 show ip bgp ipv4 unicast neighbors <идентификатор> received-routes

Отображение подробной информации о однонаправленных IPv4-маршрутах полученных от указанного узла.

Синтаксис

```
show ip bgp ipv4 unicast neighbors <идентификатор> received-routes
```

Режим ввода команды

Эксплуатационный режим.

Параметры

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения подробной информации о однонаправленных IPv4-маршрутах полученных от указанного узла.

28.4.65 show ip bgp ipv4 unicast neighbors <идентификатор> routes

Отображение подробной информации о однонаправленных IPv4-маршрутах полученных и принятых от указанного узла.

Синтаксис

```
show ip bgp ipv4 unicast neighbors <идентификатор> routes
```

Режим ввода команды

Эксплуатационный режим.

Параметры

идентификатор

IPv4- или IPv6-адрес BGP-соседа

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения подробной информации о однонаправленных IPv4-маршрутах полученных и принятых от указанного узла.

28.4.66 show ip bgp neighbors

Отображение подробной информации о узле.

Синтаксис

```
show ip bgp neighbors [<идентификатор>]
```

Режим ввода команды

Эксплуатационный режим.

Параметры

идентификатор

IPv4-адрес BGP-соседа.

Значение по умолчанию

Подробная информация о узле выводится на экран.

Указания по использованию

Эта команда используется для отображения подробной информации о узле.

28.4.67 show ip bgp neighbors <идентификатор> advertised-routes

Отображение информации о распространении маршрутов для указанного узла.

Синтаксис

```
show ip bgp neighbors <идентификатор> advertised-routes
```

Режим ввода команды

Эксплуатационный режим.

Параметры

идентификатор

IPv4-адрес BGP-соседа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения подробной информации о распространении маршрутов для указанного узла

28.4.68 show ip bgp neighbors <идентификатор> dampened-routes

Отображение информации о подавленных маршрутах указанного узла.

Синтаксис

```
show ip bgp neighbors <идентификатор> dampened-routes
```

Режим ввода команды

Эксплуатационный режим.

Параметры

идентификатор

IPv4-адрес BGP-соседа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения информации о подавленных маршрутах указанного узла.

28.4.69 show ip bgp neighbors <идентификатор> flap-statistics

Отображение статистики о нестабильности маршрута от указанного узла.

Синтаксис

```
show ip bgp neighbors <идентификатор> flap-statistics
```

Режим ввода команды

Эксплуатационный режим.

Параметры

идентификатор

IPv4-адрес BGP-соседа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения статистики о нестабильности маршрута от указанного узла.

28.4.70 show ip bgp neighbors <идентификатор> prefix-counts

Отображение информации о числе префиксов для указанного узла

Синтаксис

```
show ip bgp neighbors <идентификатор> prefix-counts
```

Режим ввода команды

Эксплуатационный режим.

Параметры

идентификатор

IPv4-адрес BGP-соседа. Возможно указание нескольких соседей, путем создания нескольких узлов конфигурации.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения информации о числе префиксов для указанного узла.

28.4.71 show ip bgp neighbors <идентификатор> received prefix-filter

Отображение подробной информации о префиксных списках от указанного узла.

Синтаксис

```
show ip bgp neighbors <идентификатор> received prefix-filter
```

Режим ввода команды

Эксплуатационный режим.

Параметры

идентификатор

IPv4- или IPv6-адрес BGP-соседа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения информации о префиксных списках от указанного узла.

28.4.72 show ip bgp neighbors <идентификатор> received-routes

Отображение подробной информации о маршрутах полученных от указанного узла.

Синтаксис

```
show ip bgp neighbors <идентификатор> received-routes
```

Режим ввода команды

Эксплуатационный режим.

Параметры

идентификатор

IPv4-адрес BGP-соседа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения информации о маршрутах полученных от указанного узла.

28.4.73 show ip bgp neighbors <идентификатор> routes

Отображение подробной информации о полученных и принятых от указанного узла.

Синтаксис

```
show ip bgp neighbors <идентификатор> routes
```

Режим ввода команды

Эксплуатационный режим.

Параметры

идентификатор

IPv4-адрес BGP-соседа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения информации о маршрутах, полученных и принятых от указанного узла.

28.4.74 show ipv6 bgp neighbors

Отображение подробной информации о узле ipv6.

Синтаксис

```
show ipv6 bgp neighbors [<идентификатор>]
```

Режим ввода команды

Эксплуатационный режим.

Параметры

идентификатор

IPv6-адрес BGP-соседа.

Значение по умолчанию

Подробная информация о узле выводится на экран.

Указания по использованию

Эта команда используется для отображения подробной информации о узле.

28.4.75 show ipv6 bgp neighbors <идентификатор> advertised-routes

Отображение информации о распространении маршрутов для указанного узла.

Синтаксис

```
show ipv6 bgp neighbors <идентификатор> advertised-routes
```

Режим ввода команды

Эксплуатационный режим.

Параметры

идентификатор

IPv6-адрес BGP-соседа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения подробной информации о распространении маршрутов для указанного узла

28.4.76 show ipv6 bgp neighbors <идентификатор> received-routes

Отображение подробной информации о однонаправленных IPv6-маршрутах, полученных от указанного узла.

Синтаксис

```
show ipv6 bgp neighbors <идентификатор> received-routes
```

Режим ввода команды

Эксплуатационный режим.

Параметры

идентификатор

IPv6-адрес BGP-соседа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения подробной информации о однонаправленных IPv6-маршрутах, полученных от указанного узла.

28.4.77 show ipv6 bgp neighbors <идентификатор> routes

Отображение подробной информации о однонаправленных IPv6-маршрутах, полученных и принятых от указанного узла.

Синтаксис

```
show ipv6 bgp neighbors <идентификатор> routes
```

Режим ввода команды

Эксплуатационный режим.

Параметры

идентификатор

IPv6-адрес BGP-соседа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения подробной информации о однонаправленных IPv6-маршрутах, полученных и принятых от указанного узла.

28.5 Отражение маршрутов BGP

Команды настройки отражения маршрутов BGP	
protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast route-reflector-client	Указание узла в качестве клиента отражателя маршрутов.
protocols bgp <номер_AC> neighbor <идентификатор> route-reflector-client	Указание локального маршрутизатора в качестве отражателя маршрутов, и обозначения узла в качестве клиента отражателя маршрутов.
protocols bgp <номер_AC> peer-group <имя_группы> address-family ipv6-unicast route-reflector-client	Указание группы узлов в качестве клиентов отражателя маршрутов.
protocols bgp <номер_AC> peer-group <имя_группы> route-reflector-client	Указание группы узлов в качестве клиентов отражателя маршрутов.
protocols bgp <номер_AC> parameters cluster-id <адрес>	Указание идентификатора (ID) BGP-кластера.
protocols bgp <номер_AC> parameters no-client-to-client-reflection	Запрещение на отражение маршрутов между отражателем маршрутов и клиентами.

28.5.1 protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast route-reflector-client

Указание узла в качестве клиента отражателя маршрутов.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast route-reflector-client

delete protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast route-reflector-client

show protocols bgp <номер_AC> neighbor <идентификатор> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        neighbor идентификатор {
            address-family {
                ipv6-unicast {
                    route-reflector-client
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

идентификатор

IPv4 или IPv6 адреса узла.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется только при одноадресатной IPv6-маршрутизации.

Форма **set** этой команды используется для настройки узла, в качестве клиента отражателя маршрутов.

Форма **delete** этой команды используется для удаления настройки.

Форма **show** этой команды используется для просмотра настройки.

28.5.2 protocols bgp <номер_AC> neighbor <идентификатор> route-reflector-client

Указание локального маршрутизатора в качестве отражателя маршрутов, и обозначение узла в качестве клиента отражателя маршрутов.

Синтаксис

```
set protocols bgp <номер_AC> neighbor <идентификатор> route-reflector-client
```

```
delete protocols bgp <номер_АС> neighbor <идентификатор> route-reflector-client

show protocols bgp <номер_АС> neighbor <идентификатор>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_АС {
        neighbor идентификатор {
            route-reflector-client
        }
    }
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных АС.

идентификатор

IPv4 или IPv6 адреса узла.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для указания локального маршрутизатора в качестве отражателя маршрутов и обозначения узла в качестве клиента отражателя маршрутов.

Форма **delete** этой команды используется для удаления узла в качестве клиента отражателя маршрутов.

Форма **show** этой команды используется для просмотра настройки узла.

28.5.3 protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast route-reflector-client

Указание группы узлов в качестве клиентов отражателя маршрутов.

Синтаксис

```
set protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast route-reflector-client

delete protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast route-reflector-client

show protocols bgp <номер_АС> peer-group <имя_группы> address-family ipv6-unicast
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_АС {
        peer-group имя_группы {
            address-family {
```

```
            ipv6-unicast {
               route-reflector-client
            }
         }
      }
   }
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных АС.

имя_группы

Обязательный. Наименование группы узлов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется только при одноадресатной IPv6-маршрутизации.

Форма **set** этой команды используется для указания группы узлов в качестве клиентов отражателя маршрутов.

Форма **delete** этой команды используется для удаления настройки.

Форма **show** этой команды используется для просмотра настройки.

28.5.4 protocols bgp <номер_АС> peer-group <имя_группы> route-reflector-client

Указание группы узлов в качестве клиентов отражателя маршрутов.

Синтаксис

```
set protocols bgp <номер_АС> peer-group <имя_группы> route-reflector-client
delete protocols bgp <номер_АС> peer-group <имя_группы> route-reflector-client
show protocols bgp <номер_АС> peer-group <имя_группы>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_АС {
      peer-group имя_группы {
         route-reflector-client
      }
   }
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных АС.

имя_группы

Наименование группы узлов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для указания группы узлов в качестве клиентов отражателя маршрутов.

Форма **delete** этой команды используется для удаления настройки.

Форма **show** этой команды используется для просмотра настройки.

28.5.5 protocols bgp <номер_АС> parameters cluster-id <адрес>

Указание идентификатора (ID) BGP-кластера.

Синтаксис

```
set protocols bgp <номер_АС> parameters cluster-id <адрес>
delete protocols bgp <номер_АС> parameters cluster-id <адрес>
show protocols bgp <номер_АС> parameters cluster-id
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_АС {
      parameters {
         cluster-id адрес
      }
   }
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных АС.

адрес

Адрес BGP-кластера.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для указания идентификатора BGP-кластера.

Форма **delete** этой команды используется для удаления BGP-кластера.

Форма **show** этой команды используется для просмотра настройки.

28.5.6 protocols bgp <номер_AC> parameters no-client-to-client-reflection

Запрещение на отражение маршрутов между отражателем маршрутов и клиентами.

Синтаксис

```
set protocols bgp <номер_AC> parameters no-client-to-client-reflection
delete protocols bgp <номер_AC> parameters no-client-to-client-reflection
show protocols bgp <номер_AC> parameters
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      parameters {
         no-client-to-client-reflection
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294. Диапазон номеров от 64512 до 65534 зарезервирован для локальных AC.

Значение по умолчанию

По умолчанию, отражение маршрутов между отражателем маршрутов и клиентами разрешено.

Указания по использованию

Форма **set** этой команды используется для запрещения отражения маршрутов между отражателем маршрутов и клиентами.

Форма **delete** этой команды используется для разрешения отражения маршрутов между отражателем маршрутов и клиентами.

Форма **show** этой команды используется для просмотра настройки.

28.6 Перераспределение маршрутов BGP

Команды настройки перераспределения IPv6-маршрутов	
protocols bgp <номер_AC> address-family ipv6-unicast redistribute connected	Перераспределение непосредственно присоединенных IPv6-маршрутов.
protocols bgp <номер_AC> address-family ipv6-unicast redistribute kernel	Перераспределение IPv6-маршрутов ядра.
protocols bgp <номер_AC> address-family ipv6-unicast redistribute ospfv3	Перераспределение IPv6-маршрутов извлеченных из протокола маршрутизации OSPFv3.
protocols bgp <номер_AC> address-family ipv6-unicast redistribute ripng	Перераспределение IPv6-маршрутов извлеченных из протокола маршрутизации ripng.
protocols bgp <номер_AC> address-family ipv6-unicast redistribute static	Перераспределение статических IPv6-маршрутов.
Команды настройки перераспределения маршрутов	
protocols bgp <номер_AC> redistribute connected	Перераспределение непосредственно присоединенных маршрутов.
protocols bgp <номер_AC> redistribute kernel	Перераспределение маршрутов ядра.

protocols bgp <номер_AC> redistribute ospf	Перераспределение маршрутов извлеченных из протокола маршрутизации OSPF.
protocols bgp <номер_AC> redistribute rip	Перераспределение маршрутов извлеченных из протокола маршрутизации RIP.
protocols bgp <номер_AC> redistribute static	Перераспределение статических маршрутов.

28.6.1 protocols bgp <номер_AC> address-family ipv6-unicast redistribute connected

Перераспределение непосредственно подключаемых IPv6-маршрутов.

Синтаксис

```
set protocols bgp <номер_AC> address-family ipv6-unicast redistribute connected [metric <метрика> | route-map <имя_карты_маршрутов>]

delete protocols bgp <номер_AC> address-family ipv6-unicast redistribute connected [metric <метрика> | route-map <имя_карты_маршрутов>]

show protocols bgp <номер_AC> address-family ipv6-unicast redistribute connected
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        address-family {
            ipv6-unicast {
                redistribute {
                    connected {
                        metric метрика
                        route-map имя_карты_маршрутов
                    }
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

метрика

Метрика применяемая к перераспределяющимся маршрутам.

имя_карты_маршрутов

Карта маршрута используемая при перераспределении маршрутов.

Значение по умолчанию

По умолчанию непосредственно подключаемые маршруты не перераспределяются.

Указания по использованию

Эта команда применяется только при одноадресатной IPv6-маршрутизации.

Форма **set** этой команды используется для перераспределения непосредственно подключаемых IPv6-маршрутов.

Форма **delete** этой команды используется для предотвращения перераспределения непосредственно подключаемых IPv6-маршрутов.

Форма **show** этой команды используется для просмотра настройки.

28.6.2 protocols bgp <номер_AC> address-family ipv6-unicast redistribute kernel

Перераспределение IPv6-маршрутов ядра.

Синтаксис

```
set protocols bgp <номер_AC> address-family ipv6-unicast redistribute kernel
[metric <метрика> | route-map <имя_карты_маршрутов>]

delete protocols bgp <номер_AC> address-family ipv6-unicast redistribute
kernel [metric <метрика> | route-map <имя_карты_маршрутов>]

show protocols bgp <номер_AC> address-family ipv6-unicast redistribute kernel
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      address-family {
         ipv6-unicast {
            redistribute {
               kernel {
                  metric метрика
                  route-map имя_карты_маршрутов
               }
            }
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

метрика

Метрика применяемая к перераспределяющимся маршрутам.

имя_карты_маршрутов

Карта маршрута используемая при перераспределении маршрутов.

Значение по умолчанию

По умолчанию маршруты не перераспределяются.

Указания по использованию

Эта команда применяется только при одноадресатной IPv6-маршрутизации.

Форма **set** этой команды используется для перераспределения IPv6-маршрутов ядра.

Форма **delete** этой команды используется для предотвращения перераспределения IPv6-маршрутов ядра.

Форма **show** этой команды используется для просмотра настройки.

28.6.3 protocols bgp <номер_AC> address-family ipv6-unicast redistribute ospfv3

Перераспределение IPv6-маршрутов извлеченных из протокола маршрутизации OSPFv3.

Синтаксис

```
set protocols bgp <номер_AC> address-family ipv6-unicast redistribute ospfv3
[metric <метрика> | route-map <имя_карты_маршрутов>]

delete protocols bgp <номер_AC> address-family ipv6-unicast redistribute
ospfv3 [metric <метрика> | route-map <имя_карты_маршрутов>]

show protocols bgp <номер_AC> address-family ipv6-unicast redistribute ospfv3
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      address-family {
         ipv6-unicast {
            redistribute {
               ospfv3{
                  metric метрика
                  route-map имя_карты_маршрутов
               }
            }
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

метрика

Метрика применяемая к перераспределяющимся маршрутам.

имя_карты_маршрутов

Карта маршрута используемая при перераспределении маршрутов.

Значение по умолчанию

По умолчанию маршруты не перераспределяются.

Указания по использованию

Эта команда применяется только при одноадресатной IPv6-маршрутизации.

Форма **set** этой команды используется для перераспределения IPv6-маршрутов извлеченных из протокола маршрутизации OSPFv3.

Форма **delete** этой команды используется для предотвращения IPv6-маршрутов извлеченных из протокола маршрутизации OSPFv3.

Форма **show** этой команды используется для просмотра настройки.

28.6.4 protocols bgp <номер_AC> address-family ipv6-unicast redistribute ripng

Перераспределение IPv6-маршрутов извлеченных из протокола маршрутизации ripng.

Синтаксис

```
set protocols bgp <номер_AC> address-family ipv6-unicast redistribute ripng [metric <метрика> | route-map <имя_карты_маршрутов>]

delete protocols bgp <номер_AC> address-family ipv6-unicast redistribute ripng [metric <метрика> | route-map <имя_карты_маршрутов>]

show protocols bgp <номер_AC> address-family ipv6-unicast redistribute ripng
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        address-family {
            ipv6-unicast {
                redistribute {
                    ripng {
                        metric метрика
                        route-map имя_карты_маршрутов
                    }
                }
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

метрика

Метрика применяемая к перераспределяющимся маршрутам.

имя_карты_маршрутов

Карта маршрута используемая при перераспределении маршрутов.

Значение по умолчанию

По умолчанию маршруты не перераспределяются.

Указания по использованию

Эта команда применяется только при одноадресатной IPv6-маршрутизации.

Форма **set** этой команды используется для перераспределения IPv6-маршрутов извлеченных из протокола маршрутизации ripng.

Форма **delete** этой команды используется для предотвращения IPv6-маршрутов извлеченных из протокола маршрутизации ripng.

Форма **show** этой команды используется для просмотра настройки.

28.6.5 protocols bgp <номер_AC> address-family ipv6-unicast redistribute static

Перераспределение статических IPv6-маршрутов.

Синтаксис

```
set protocols bgp <номер_AC> address-family ipv6-unicast redistribute static [metric <метрика> | route-map <имя_карты_маршрутов>]

delete protocols bgp <номер_AC> address-family ipv6-unicast redistribute static [metric <метрика> | route-map <имя_карты_маршрутов>]

show protocols bgp <номер_AC> address-family ipv6-unicast redistribute static
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      address-family {
         ipv6-unicast {
            redistribute {
               static {
                  metric метрика
                  route-map имя_карты_маршрутов
               }
            }
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

метрика

Метрика применяемая к перераспределяющимся маршрутам.

имя_карты_маршрутов

Карта маршрута используемая при перераспределении маршрутов.

Значение по умолчанию

По умолчанию маршруты не перераспределяются.

Указания по использованию

Эта команда применяется только при одноадресатной IPv6-маршрутизации.

Форма **set** этой команды используется для перераспределения статических IPv6-маршрутов.

Форма **delete** этой команды используется для предотвращения перераспределения статических IPv6-маршрутов.

Форма **show** этой команды используется для просмотра настройки.

28.6.6 protocols bgp <номер_AC> redistribute connected

Перераспределение непосредственно присоединенных маршрутов.

Синтаксис

```
set protocols bgp <номер_AC> redistribute connected [metric <метрика> | route-map <имя_карты_маршрутов>]

delete protocols bgp <номер_AC> redistribute connected [metric <метрика> | route-map <имя_карты_маршрутов>]

show protocols bgp <номер_AC> redistribute connected
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        redistribute {
            connected {
                metric метрика
                route-map имя_карты_маршрутов
            }
        }
    }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

метрика

Метрика применяемая к перераспределяющимся маршрутам.

имя_карты_маршрутов

Карта маршрута используемая при перераспределении маршрутов.

Значение по умолчанию

По умолчанию маршруты не перераспределяются.

Указания по использованию

Форма **set** этой команды используется для перераспределения непосредственно подключаемых маршрутов.

Форма **delete** этой команды используется для предотвращения перераспределения непосредственно подключаемых маршрутов.

Форма **show** этой команды используется для просмотра настройки.

28.6.7 protocols bgp <номер_AC> redistribute kernel

Перераспределение IPv6-маршрутов ядра.

Синтаксис

```
set protocols bgp <номер_AC> redistribute kernel [metric <метрика> | route-map <имя_карты_маршрутов>]

delete protocols bgp <номер_AC> redistribute kernel [metric <метрика> | route-map <имя_карты_маршрутов>]
```

```
show protocols bgp <номер_AC> redistribute kernel
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      redistribute {
         kernel {
            metric метрика
            route-map имя_карты_маршрутов
         }
      }
   }
}
```

Параметры

номер_AC

Уникальный номер, который присваивается каждой AC при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

метрика

Метрика применяемая к перераспределяющимся маршрутам.

имя_карты_маршрутов

Карта маршрута используемая при перераспределении маршрутов.

Значение по умолчанию

По умолчанию маршруты не перераспределяются.

Указания по использованию

Форма **set** этой команды используется для перераспределения маршрутов ядра.

Форма **delete** этой команды используется для предотвращения перераспределения маршрутов ядра.

Форма **show** этой команды используется для просмотра настройки.

28.6.8 protocols bgp <номер_AC> redistribute ospf

Перераспределение маршрутов извлеченных из протокола маршрутизации OSPF.

Синтаксис

```
set protocols bgp <номер_AC> redistribute ospf [metric <метрика> | route-map <имя_карты_маршрутов>]

delete protocols bgp <номер_AC> redistribute ospf [metric <метрика> | route-map <имя_карты_маршрутов>]

show protocols bgp <номер_AC> redistribute ospf
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      redistribute {
```

```
            ospf {
               metric метрика
               route-map имя_карты_маршрутов
            }
         }
      }
   }
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

метрика

Метрика применяемая к перераспределяющимся маршрутам.

имя_карты_маршрутов

Карта маршрута используемая при перераспределении маршрутов.

Значение по умолчанию

По умолчанию маршруты не перераспределяются.

Указания по использованию

Форма **set** этой команды используется для перераспределения маршрутов извлеченных из протокола маршрутизации OSPF.

Форма **delete** этой команды используется для предотвращения маршрутов извлеченных из протокола маршрутизации OSPF.

Форма **show** этой команды используется для просмотра настройки.

28.6.9 protocols bgp <номер_АС> redistribute rip

Перераспределение маршрутов извлеченных из протокола маршрутизации RIP.

Синтаксис

```
set protocols bgp <номер_АС> redistribute rip [metric <метрика> | route-map <имя_карты_маршрутов>]

delete protocols bgp <номер_АС> redistribute rip [metric <метрика> | route-map <имя_карты_маршрутов>]

show protocols bgp <номер_АС> redistribute rip
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_АС {
      redistribute {
         rip {
            metric метрика
            route-map имя_карты_маршрутов
         }
      }
   }
```

```
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

метрика

Метрика применяемая к перераспределяющимся маршрутам.

имя_карты_маршрутов

Карта маршрута используемая при перераспределении маршрутов.

Значение по умолчанию

По умолчанию маршруты не перераспределяются.

Указания по использованию

Форма **set** этой команды используется для перераспределения маршрутов извлеченных из протокола маршрутизации RIP.

Форма **delete** этой команды используется для предотвращения маршрутов извлеченных из протокола маршрутизации RIP.

Форма **show** этой команды используется для просмотра настройки.

28.6.10 protocols bgp <номер_АС> redistribute static

Перераспределение статических маршрутов.

Синтаксис

```
set protocols bgp <номер_АС> redistribute static [metric <метрика> | route-map <имя_карты_маршрутов>]

delete protocols bgp <номер_АС> redistribute static [metric <метрика> | route-map <имя_карты_маршрутов>]

show protocols bgp <номер_АС> redistribute static
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_АС {
        redistribute {
            static {
                metric метрика
                route-map имя_карты_маршрутов
            }
        }
    }
}
```

Параметры

номер_АС

Уникальный номер, который присваивается каждой АС при использовании в BGP маршрутизации. Значение должно лежать в диапазоне от 1 до 4294967294.

метрика

Метрика, применяемая к перераспределяющимся маршрутам.

имя_карты_маршрутов

Карта маршрута используемая при перераспределении маршрутов.

Значение по умолчанию

По умолчанию маршруты не перераспределяются.

Указания по использованию

Форма **set** этой команды используется для перераспределения статических маршрутов.

Форма **delete** этой команды используется для предотвращения перераспределения статических маршрутов.

Форма **show** этой команды используется для просмотра настройки.

28.7 Команды BGP

Режим настройки	
Глобальные настройки BGP	
protocols bgp <номер_АС>	Создание узла конфигурации BGP и указание АС принадлежности для данного маршрутизатора.
protocols bgp <номер_АС> aggregate-address <подсеть_ipv4>	Указание IPv4-подсети для осуществления агрегирования маршрутов, входящих в неё.
protocols bgp <номер_АС> network <подсеть_ipv4>	Указание IPv4-подсети для объявления другим узлам BGP.
protocols bgp <номер_АС> timers	Установка глобальных таймеров BGP.
Глобальные настройки BGP - IPv6	
protocols bgp <номер_АС> address-family ipv6-unicast	Создание узла конфигурации однонаправленных IPv6-маршрутов BGP .
protocols bgp <номер_АС> address-family ipv6-unicast aggregate-address <подсеть_ipv6>	Указание IPv6-подсети для осуществления агрегирования маршрутов, входящих в неё.
protocols bgp <номер_АС> address-family ipv6-unicast network <подсеть_ipv6>	Указание IPv6-подсети для объявления другим узлам BGP.
Тонкие настройки маршрутизатора BGP	
protocols bgp <номер_АС> parameters always-compare-med	Включение или отключение сравнения атрибутов MED (MULTI_EXIT_DISC) для путей, полученных от соседних узлов, находящихся в разных АС.
protocols bgp <номер_АС> parameters bestpath as-path	Настройка условий сравнения пути АС в процессе выбора наилучшего пути.
protocols bgp <номер_АС> parameters bestpath compare-routerid	Настройка сравнения BGP ID в процессе выбора наилучшего пути при получении двух одинаковых маршрутов от разных узлов.
protocols bgp <номер_АС> parameters bestpath med	Настройка сравнения атрибута MED в процессе выбора наилучшего пути для путей, полученных от узлов, состоящих в конфедерации.
protocols bgp <номер_АС> parameters dampening	Включение или отключения демпфирования колебаний маршрутов и установка параметров демпфирования.
protocols bgp <номер_АС> parameters default	Установка параметров маршрутизации BGP, используемых по умолчанию.
protocols bgp <номер_АС> parameters deterministic-med	Включение или отключение внедрения детерминированного MED.
protocols bgp <номер_АС> parameters distance global	Указание глобальной административной дистанции для всех маршрутов BGP.
protocols bgp <номер_АС> parameters distance prefix <подсеть> distance <дистанция>	Указание административной дистанции для маршрутов BGP для указанного префикса назначения.
protocols bgp <номер_АС> parameters disable-network-import-check	Запрет проверки маршрутов IGP на наличие префикса в таблице маршрутизации.

protocols bgp <номер_AC> parameters enforce-first-as	Включение или отключение принудительной подстановки номеров AC в начало атрибута AS_PATH во всех входящих обновлениях для узлов eBGP.
protocols bgp <номер_AC> parameters graceful-restart	Включение или отключение мягкого перезапуска процесса BGP.
protocols bgp <номер_AC> parameters log-neighbor-changes	Включение журналирования изменения состояния соседних узлов BGP.
protocols bgp <номер_AC> parameters no-fast-external-failover	Запрет автоматического перезапуска сессии BGP при разрыве соединения с соседним узлом BGP.
protocols bgp <номер_AC> parameters router-id <идентификатор>	Указание BGP ID для данного маршрутизатора.
protocols bgp <номер_AC> parameters scan-time <время>	Указание временного интервала между отправкой запроса на предоставление маршрутной информации по протоколу BGP.
Эксплуатационный режим	
clear ip bgp <адрес>	Сброс соединения BGP с указанным соседним узлом.
clear ip bgp <адрес> ipv4 unicast	Сброс однонаправленного IPv4 соединения BGP.
clear ip bgp dampening	Очистка информации о демпфировании колебаний маршрутов с восстановлением всех подавленных маршрутов.
routing bgp debug enable	Включение или отключения создания отладочного сообщения при возникновении события присвоения BGP ID, получения или отправки сообщения BGP.
routing bgp debug disable	Отключение записи отладочной информации протокола BGP
routing bgp debug enable events	Включение или отключения создания отладочного сообщения при возникновении событий BGP.
routing bgp debug enable filters	Включение или отключения создания отладочного сообщения при возникновении событий, связанных с фильтрами BGP.
routing bgp debug enable fsm	Включение или отключения создания отладочного сообщения при возникновении событий, связанных машиной конечных состояний (FSM) BGP.
routing bgp debug enable keepalives	Включение или отключения создания отладочного сообщения при возникновении событий, связанных с отправкой и получением сообщений keep-alive.
routing bgp debug enable updates	Отображение отладочной информации, связанной с обновлениями маршрутов BGP.
routing bgp debug enable zebra	Отображение отладочной информации, связанной с настройками демона Zebra BGP.
routing bgp debug status	Отображение отладочных флагов протокола BGP.
show ip bgp	Отображение маршрутов BGP.
show ip bgp attribute-info	Отображение информации об атрибутах сети BGP.
show ip bgp cidr-only	Отображение маршрутов BGP с бесклассовой адресацией.
show ip bgp community <сообщество>	Отображение маршрутов, принадлежащих определённым сообществам BGP.
show ip bgp community-info	Отображение информации о сообществе BGP.
show ip bgp community-list <список_сообществ>	Отображение маршрутов, принадлежащих сообществам из определённого списка сообществ BGP.
show ip bgp dampened-paths	Отображение текущего перечня подавленных маршрутов BGP.
show ip bgp filter-list <список_путей_ac>	Отображение маршрутов BGP, входящих в список путей AC.
show ip bgp flap-statistics	Отображение статистики колебания маршрутов BGP.
show ip bgp flap-statistics cidr-only	Отображение статистики колебания маршрутов BGP для маршрутов с бесклассовой адресацией.
show ip bgp flap-statistics filter-list <список_путей_ac>	Отображение статистики колебания маршрутов BGP для маршрутов, входящих в определённый список путей AC.

show ip bgp flap-statistics prefix-list <список_префиксов>	Отображение статистики колебания маршрутов BGP для маршрутов с адресом, совпадающим с адресами из определённого списка префиксов.
show ip bgp flap-statistics regexp <регулярное_выражение>	Отображение статистики колебания маршрутов BGP для маршрутов содержащих указанное регулярное выражение.
show ip bgp flap-statistics route-map <имя_карты_маршрутов>	Отображение статистики колебания маршрутов BGP для маршрутов с адресом, входящим в определённую карту маршрутов.
show ip bgp ipv4 unicast	Отображение информации об однонаправленных IPv4-маршрутах.
show ip bgp ipv4 unicast cidr-only	Отображение информации об однонаправленных IPv4-маршрутах.
show ip bgp ipv4 unicast community <сообщество>	Отображение однонаправленных IPv4-маршрутов BGP, принадлежащих определённому сообществу BGP.
show ip bgp ipv4 unicast community-list <список_сообществ>	Отображение однонаправленных IPv4-маршрутов, принадлежащих сообществам из определённого списка сообществ BGP.
show ip bgp ipv4 unicast filter-list <список_путей_ас>	Отображение однонаправленных IPv4-маршрутов BGP, входящих в список путей АС.
show ip bgp ipv4 unicast neighbors	Отображение информации об однонаправленных IPv4-соединениях с соседними узлами BGP.
show ip bgp ipv4 unicast paths	Отображение информации об однонаправленных IPv4 путях BGP.
show ip bgp ipv4 unicast prefix-list <список_префиксов>	Отображение перечня однонаправленных IPv4-маршрутов, адреса которых совпадают с адресами из определённого списка префиксов.
show ip bgp ipv4 unicast regexp <регулярное_выражение>	Отображение однонаправленных IPv4-маршрутов BGP, содержащих указанное регулярное выражение.
show ip bgp ipv4 unicast route-map <имя_карты_маршрутов>	Отображение однонаправленных IPv4-маршрутов BGP с адресами, входящими в определённую карту маршрутов.
show ip bgp ipv4 unicast statistics	Отображение статистики для однонаправленных IPv4-маршрутов BGP.
show ip bgp ipv4 unicast summary	Отображение краткой информации об однонаправленных IPv4-маршрутов BGP.
show ip bgp neighbors	Отображение информации о соседних узлах BGP.
show ip bgp memory	Отображение информации об объёме памяти, используемой процессом BGP.
show ip bgp paths	Отображение путей BGP.
show ip bgp prefix-list <список_префиксов>	Отображение перечня путей BGP, префиксы которых совпадают с префиксами из определённого списка префиксов.
show ip bgp regexp <регулярное_выражение>	Отображение маршрутов BGP, содержащих указанное регулярное выражение.
show ip bgp route-map <имя_карты_маршрутов>	Отображение маршрутов BGP, входящих в указанную карту маршрутов.
show ip bgp rsclient <адрес_узла>	Отображение маршрутов BGP, входящих в информационную базу маршрутизации.
show ip bgp scan	Отображение статуса сети BGP.
show ip bgp summary	Отображение краткой информации о сети BGP.
show ip route bgp	Отображение маршрутов BGP.
show ipv6 bgp	Отображение маршрутов BGP.
show ipv6 bgp community <сообщество>	Отображение маршрутов BGP, принадлежащих определённому сообществу BGP.
show ipv6 bgp community-list <список_сообществ>	Отображение маршрутов, принадлежащих сообществам из определённого списка сообществ BGP.

show ipv6 bgp filter-list <список_путей_ac>	Отображение маршрутов BGP, входящих в список путей AC.
show ipv6 bgp neighbor	Отображение информации о соседних узлах BGP.
show ipv6 bgp prefix-list <список_префиксов>	Отображение перечня путей BGP, префиксы которых совпадают с префиксами из определённого списка префиксов.
show ipv6 bgp regexp <регулярное_выражение>	Отображение маршрутов BGP, содержащих указанное регулярное выражение.
show ipv6 bgp summary	Отображение краткой информации о сети BGP.

28.7.1 protocols bgp <номер_AC>

Создание узла конфигурации BGP и указание AC принадлежности для данного маршрутизатора.

Синтаксис

```
set protocols bgp <номер_AC>
delete protocols bgp <номер_AC>
show protocols bgp <номер_AC>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC
}
```

Параметры

номер_AC

Номер AC в которой находится данный маршрутизатор. Значение должно лежать в диапазоне от 1 до 4294967296.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для создания узла конфигурации BGP и указания AC принадлежности для данного маршрутизатора.

Форма **set** данной команды используется для создания узла конфигурации BGP и указания AC принадлежности для данного маршрутизатора.

Форма **delete** данной команды используется для удаления узла конфигурации BGP и исключения данного маршрутизатора из AC с указанным номером.

Форма **show** данной команды используется для отображения текущей конфигурации в данном контексте.

28.7.2 protocols bgp <номер_AC> aggregate-address <подсеть_ipv4>

Указание IPv4-подсети для осуществления агрегирования маршрутов, входящих в неё.

Синтаксис

```
set protocols bgp <номер_AC> aggregate-address <подсеть_ipv4> [as-set | summary-only]
delete protocols bgp <номер_AC> aggregate-address <подсеть_ipv4>
show protocols bgp <номер_AC> aggregate-address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
```

```
    bgp номер_AC {
        aggregate-address подсеть_ipv4 {
            as-set
            summary-only
        }
    }
}
```

Параметры

номер_AC

Номер AC в которой находится данный маршрутизатор.

подсеть_ipv4

Подсеть IPv4, маршруты которой будут агрегированы. Используется формат ip-адрес/префикс.

as-set

При включении данного параметра, атрибут пути AC маршрута, полученного в результате агрегирования, будет включать в себя номера AC всех суммируемых маршрутов. По умолчанию путь AC суммарного маршрута содержит только номер AC, в которой состоит

маршрутизатор, анонсировавший данный маршрут.

summary-only

При включении данного параметра, маршрутизатор анонсирует только маршрут, полученный в результате агрегирования (суммарный маршрут), но не анонсирует его компоненты. По умолчанию анонсируется как суммарный маршрут, так и его компоненты.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для осуществления агрегации маршрутов, входящих в указанную подсеть, для последующего анонсирования суммарного маршрута. В данной команде возможно использование параметров summary-only и as-set одновременно. В таком случае маршрутизатор будет анонсировать только суммарный маршрут, но при этом путь AC этого маршрута будет содержать номера AC всех суммируемых маршрутов.

Форма **set** данной команды используется для указания определённого диапазона IPv4-адресов для осуществления их агрегации.

Форма **delete** данной команды используется для удаления агрегированных адресов.

Форма **show** данной команды используется для отображения текущей конфигурации в данном контексте.

28.7.3 protocols bgp <номер_AC> network <подсеть_ipv4>

Указание IPv4-подсети для объявления другим узлам BGP.

Синтаксис

```
set protocols bgp <номер_AC> network <подсеть_ipv4> [backdoor | route-map <имя_карты_маршрутов>]

delete protocols bgp <номер_AC> network <подсеть_ipv4> [backdoor | route-map]

show protocols bgp <номер_AC> network
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
```

```
        network подсеть_ipv4 {
           backdoor
           route-map имя_карты_маршрутов
        }
     }
  }
```

Параметры

номер_AC

Номер AC в которой находится данный маршрутизатор.

подсеть_ipv4

Множественный узел. Подсеть IPv4 для объявления другим узлам посредством процесса маршрутизации BGP. Используется формат ip-адрес/префикс.

Для указания нескольких подсетей необходимо создать соответствующее количество узлов конфигурации network.

backdoor

Указанная подсеть считается достижимой посредством backdoor маршрута. Backdoor сеть считается локальной сетью и не анонсируется другим узлам.

имя_карты_маршрутов

Имя карты маршрутов, используемой при объявлении указанной подсети.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания подсети, которая будет объявляться другим узлам посредством протокола BGP. Следует учитывать, что указанная в данном узле конфигурации подсеть будет сразу объявлена всем BGP соседям вне зависимости от наличия или отсутствия соответствующих маршрутов в таблице маршрутизации изделия.

Форма **set** данной команды используется для указания подсети для протокола BGP.

Форма **delete** данной команды используется для удаления подсети протокола BGP.

Форма **show** данной команды используется для отображения текущей конфигурации в данном контексте.

28.7.4 protocols bgp <номер_AC> timers

Установка глобальных таймеров BGP.

Синтаксис

```
set protocols bgp <номер_AC> timers [keepalive <время> | holdtime <время>]
delete protocols bgp <номер_AC> timers [keepalive | holdtime]
show protocols bgp <номер_AC> timers [keepalive | holdtime]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      timers {
         keepalive время
         holdtime время
```

```
        }
    }
}
```

Параметры

номер_AC

Номер AC в которой находится данный маршрутизатор.

keepalive *время*

Периодичность (в секундах) отправки сообщения keepalive соседям BGP. Значение должно лежать в диапазоне от 1 до 65535. По умолчанию установлено значение 60.

holdtime *время*

Время (в секундах) после последнего полученного пакета поддержания соединения (keepalive) от определённого узла BGP, по истечению которого соединение с данным узлом считается разорванным. Поддерживаются значение 0 и значения в диапазоне от 4 до 65535. Установка значения 0 отключает данный таймер. По умолчанию установлено значение 180.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для установки глобальных таймеров BGP. Эти таймеры используются для мониторинга состояния других узлов BGP, подключенных к данному маршрутизатору. Установленные значения действительны для всех узлов BGP в сети, за исключением узлов, в настройках которых указаны собственные значения. Таймеры, конкретно заданные для определённого узла отменяют глобальные таймеры.

Форма **set** данной команды используется для установки глобальных таймеров BGP.

Форма **delete** данной команды используется для установки значений, указанных по умолчанию для каждого таймера.

Форма **show** данной команды используется для отображения текущей конфигурации в данном контексте.

28.7.5 protocols bgp <номер_AC> address-family ipv6-unicast

Создание узла конфигурации однонаправленных IPv6-маршрутов BGP .

Синтаксис

```
set protocols bgp <номер_AC> address-family ipv6-unicast
delete protocols bgp <номер_AC> address-family ipv6-unicast
show protocols bgp <номер_AC> address-family ipv6-unicast
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      address-family {
         ipv6-unicast
      }
   }
}
```

Параметры

номер_AC

Номер AC в которой находится данный маршрутизатор.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для создания узла конфигурации BGP для протокола IPv6, что позволяет включить использовать BGP поверх IPv6 в Numa edge.

Форма **set** данной команды используется для создания узла конфигурации однонаправленных маршрутов BGP поверх IPv6.

Форма **delete** данной команды используется для узла конфигурации однонаправленных маршрутов BGP поверх IPv6.

Форма **show** данной команды используется для отображения текущей конфигурации в данном контексте.

28.7.6 protocols bgp <номер_AC> address-family ipv6-unicast aggregate-address <подсеть_ipv6>

Указание IPv6-подсети для осуществления агрегирования маршрутов, входящих в неё.

Синтаксис

```
set protocols bgp <номер_AC> address-family ipv6-unicast aggregate-address <подсеть_ipv6> [summary-only]

delete protocols bgp <номер_AC> address-family ipv6-unicast aggregate-address <подсеть_ipv6>

show protocols bgp <номер_AC> address-family ipv6-unicast aggregate-address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      address-family {
         ipv6-unicast {
            aggregate-address подсеть_ipv6 {
               summary-only
            }
         }
      }
   }
}
```

Параметры

номер_AC

Номер AC в которой находится данный маршрутизатор.

подсеть_ipv6

Подсеть IPv6, маршруты которой будут агрегированы.

summary-only

При включении данного параметра, маршрутизатор анонсирует только маршрут, полученный в результате агрегирования (суммарный маршрут), но не анонсирует его компоненты. По умолчанию анонсируется как суммарный маршрут, так и его компоненты.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для осуществления агрегации маршрутов, входящих в указанную подсеть, для последующего анонсирования суммарного маршрута. Эта команда применима только к однонаправленным маршрутам IPv6.

Форма **set** данной команды используется для указания определённого диапазона IPv6-адресов для осуществления их агрегации.

Форма **delete** данной команды используется для удаления агрегированных адресов.

Форма **show** данной команды используется для отображения текущей конфигурации в данном контексте.

28.7.7 protocols bgp <номер_AC> address-family ipv6-unicast network <подсеть_ipv6>

Указание IPv6-подсети для объявления другим узлам BGP.

Синтаксис

```
set protocols bgp <номер_AC> address-family ipv6-unicast network <подсеть_ipv6>

delete protocols bgp <номер_AC> address-family ipv6-unicast network <подсеть_ipv6>

show protocols bgp <номер_AC> address-family ipv6-unicast network <подсеть_ipv6>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      address-family {
         ipv6-unicast {
            network подсеть_ipv6
         }
      }
   }
}
```

Параметры

номер_AC

Номер AC в которой находится данный маршрутизатор.

подсеть_ipv6

Множественный узел. Подсеть IPv6 для объявления другим узлам посредством процесса маршрутизации BGP. Используется формат ipv6-адрес/префикс.

Для указания нескольких подсетей необходимо создать соответствующее количество узлов конфигурации network.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания подсети, которая будет объявляться другим узлам посредством протокола BGP. Эта команда применима только к однонаправленным маршрутам IPv6.

Форма **set** данной команды используется для указания подсети для протокола BGP.

Форма **delete** данной команды используется для удаления подсети протокола BGP.

Форма **show** данной команды используется для отображения текущей конфигурации в данном контексте.

28.7.8 protocols bgp <номер_AC> parameters always-compare-med

Включение или отключение сравнения атрибутов MED (MULTI_EXIT_DISC) для путей, полученных от соседних узлов, находящихся в разных AC.

Синтаксис

```
set protocols bgp <номер_AC> parameters always-compare-med
delete protocols bgp <номер_AC> parameters always-compare-med
show protocols bgp <номер_AC> parameters
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      parameters {
         always-compare-med
      }
   }
}
```

Параметры

номер_AC

Номер AC в которой находится данный маршрутизатор. Значение должно лежать в диапазоне от 1 до 4294967296.

Значение по умолчанию

Отсутствует (сравнение атрибутов MED не производится).

Указания по использованию

Данная команда используется для включения или отключения сравнения атрибутов MED (Multi Exit Discriminator) для путей, полученных от соседних узлов, находящихся в разных автономных системах. Сравнение по данному атрибуту производится только в том случае, если сравниваемые маршруты имеют одинаковый путь AC.

Форма **set** данной команды используется для включения сравнения атрибутов MED.

Форма **delete** данной команды используется для отключения сравнения атрибутов MED.

Форма **show** данной команды используется для отображения текущей конфигурации в данном контексте.

28.7.9 protocols bgp <номер_AC> parameters bestpath as-path

Настройка условий сравнения пути AC в процессе выбора наилучшего пути.

Синтаксис

```
set protocols bgp <номер_AC> parameters bestpath as-path [confed | ignore]
delete protocols bgp <номер_AC> parameters bestpath as-path
show protocols bgp <номер_AC>  parameters bestpath
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
```

```
        parameters {
            bestpath {
                as-path {
                    confed
                    ignore
                }
            }
        }
    }
}
```

Параметры

номер_AC

Номер AC в которой находится данный маршрутизатор. Значение должно лежать в диапазоне от 1 до 4294967296.

confed

Использование сравнения путей AC в рамках конфедерации в процессе выбора наилучшего пути.

ignore

Запрет сравнения атрибутов AS_PATH в процессе выбора наилучшего пути.

Значение по умолчанию

Отсутствует (сравнение атрибутов AS_PATH внутри конфедерации не производится, при этом отсутствует запрет сравнения атрибутов AS_PATH в процессе выбора наилучшего пути).

Указания по использованию

Форма **set** данной команды используется для настройки условий сравнения пути AC в процессе выбора наилучшего пути.

Форма **delete** данной команды используется для установки условий выбора наилучшего пути, принятых по умолчанию.

Форма **show** данной команды используется для отображения настройки условий выбора наилучшего пути.

28.7.10 protocols bgp <номер_AC> parameters bestpath compare-routerid

Настройка сравнения BGP ID в процессе выбора наилучшего пути при получении двух одинаковых маршрутов от разных узлов.

Синтаксис

```
set protocols bgp <номер_AC> parameters bestpath compare-routerid
delete protocols bgp <номер_AC> parameters bestpath compare-routerid
show protocols bgp <номер_AC> parameters bestpath
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        parameters {
            bestpath {
                compare-routerid
            }
```

```
        }
    }
}
```

Параметры

номер_AC

Номер AC в которой находится данный маршрутизатор. Значение должно лежать в диапазоне от 1 до 4294967296.

Значение по умолчанию

Отсутствует (по умолчанию, маршрутизатор не производит сравнение двух одинаковых маршрутов, полученных от разных узлов).

Указания по использованию

Эта команда используется для настройки сравнения BGP ID в процессе выбора наилучшего пути при получении двух одинаковых маршрутов от разных узлов.

Форма **set** данной команды используется для включения сравнения BGP ID в процессе выбора наилучшего пути при получении двух одинаковых маршрутов от разных узлов.

Форма **delete** данной команды используется для отключения сравнения BGP ID в процессе выбора наилучшего пути при получении двух одинаковых маршрутов от разных узлов.

Форма **show** данной команды используется для отображения настройки условий выбора наилучшего пути.

28.7.11 protocols bgp <номер_AC> parameters bestpath med

Настройка сравнения атрибута MED в процессе выбора наилучшего пути для путей, полученных от узлов, состоящих в конфедерации.

Синтаксис

```
set protocols bgp <номер_AC> parameters bestpath med [confed | missing-as-worst]
```

```
delete protocols bgp <номер_AC> parameters bestpath med [confed | missing-as-worst]
```

```
show protocols bgp <номер_AC> parameters bestpath
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      parameters {
         bestpath {
            med {
               confed
               missing-as-worst
            }
         }
      }   }}
```

Параметры

номер_AC

Номер AC в которой находится данный маршрутизатор. Значение должно лежать в диапазоне от 1 до 4294967296.

confed

Использование сравнения атрибута MED в рамках конфедерации в процессе выбора наилучшего пути.

missing-as-worst

Путь с отсутствующим атрибутом MED считается наименее предпочтительным.

Значение по умолчанию

Отсутствует (по умолчанию, маршрутизатор не производит сравнение атрибутов MED в рамках процесса выбора наилучшего пути).

Указания по использованию

Эта команда используется для настройки сравнения атрибута MED в процессе выбора наилучшего пути для путей, полученных от узлов, состоящих в конфедерации.

Форма **set** данной команды используется для включения сравнения атрибута MED для узлов, состоящих в конфедерации, в процессе выбора наилучшего пути.

Форма **delete** данной команды используется для включения сравнения атрибута MED для узлов, состоящих в конфедерации, в процессе выбора наилучшего пути.

Форма **show** данной команды используется для отображения настройки условий выбора наилучшего пути.

28.7.12 protocols bgp <номер_AC> parameters dampening

Включение или отключения демпфирования колебаний маршрутов и установка параметров демпфирования.

Синтаксис

```
set protocols bgp <номер_AC> parameters dampening [half-life <время> | re-use <время> | start-suppress-time <время> | max-suppress-time <время>]

delete protocols bgp <номер_AC> parameters dampening [half-life | re-use | start-suppress-time | max-suppress-time]

show protocols bgp <номер_AC> parameters dampening
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        parameters {
            dampening {
                half-life время
                max-suppress-time время
                re-use время
                start-suppress-time время
            }
        }
    }
}
```

Параметры

номер_AC

Номер AC в которой находится данный маршрутизатор. Значение должно лежать в диапазоне от 1 до 4294967296.

half-life *время*

Промежуток времени (в секундах), по истечении которого значение параметра **suppress** уменьшается в два раза. Значение должно лежать в диапазоне от 1 до 45. По умолчанию установлено значение, равное 15.

max-suppress-time *время*

Максимальное значение промежутка времени (в секундах), в течении которого маршрут может быть подавлен (suppressed). Значение должно лежать в диапазоне от 1 до 255. По умолчанию установлено значение, равное 60.

re-use *время*

Если значение параметра **suppress** меньше установленного значения параметра **re-use**, то данный маршрут перестаёт считаться подавленным. Значение должно лежать в диапазоне от 1 до 20000. По умолчанию установлено значение равное 750.

start-suppress-time *время*

Если значение параметра **suppress** маршрута превысит значение данного параметра, то колеблющийся маршрут будет подавлен. Значение должно лежать в диапазоне от 1 до 20000. По умолчанию установлено значение равное 2000.

Значение по умолчанию

Отсутствует (демпфирование колебаний маршрутов отключено).

Указания по использованию

Эта команда используется для включения или отключения функции демпфирования колебаний маршрутов, а также для установки параметров демпфирования.

Форма **set** данной команды используется для настройки параметров демпфирования колебаний маршрутов, либо для включения демпфирования колебаний маршрутов со значениями параметров по умолчанию.

Форма **delete** данной команды используется для восстановления значений параметров демпфирования колебаний маршрутов, указанных по умолчанию, либо для отключения демпфирования колебаний маршрутов.

Форма **show** данной команды используется для отображения настройки демпфирования колебаний маршрутов.

28.7.13 protocols bgp <номер_AC> parameters default

Установка параметров маршрутизации BGP, используемых по умолчанию.

Синтаксис

```
set protocols bgp <номер_AC> parameters default [local-pref <предпочтительность> | no-ipv4-unicast]

delete protocols bgp <номер_AC> parameters default [local-pref <предпочтительность> | no-ipv4-unicast]

show protocols bgp <номер_AC> parameters default
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_AC {
        parameters {
            default {
                local-pref предпочтительность
                no-ipv4-unicast
            }
        }
    }
```

```
}
```

Параметры

номер_AC

Номер AC в которой находится данный маршрутизатор. Значение должно лежать в диапазоне от 1 до 4294967296.

предпочтительность

Определение вероятность выбора локальных маршрутов в процессе выбора наилучшего пути для узлов iBGP. Чем больше значение данного параметра, тем больше вероятность выбора локального маршрута. Значение должно лежать в диапазоне от 0 до 4294967295. По умолчанию установлено значение 100.

no-ipv4-unicast

Запрет на использование однонаправленных IPv4-адресов в качестве адресов, используемых по умолчанию для установки соединений BGP.

Значение по умолчанию

значение атрибута local-pref равно 100, однонаправленные адреса IPv4 используются в качестве адресом по умолчанию для установки соединения BGP.

Указания по использованию

Форма **set** данной команды применяется для установки параметров маршрутизации BGP, используемых по умолчанию.

Форма **delete** данной команды используется для восстановления значения, указанного по умолчанию.

Форма **show** данной команды используется для отображения текущей конфигурации в данном контексте.

28.7.14 protocols bgp <номер_AC> parameters deterministic-med

Включение или отключение внедрения детерминированного MED.

Синтаксис

```
set protocols bgp <номер_AC> parameters deterministic-med
delete protocols bgp <номер_AC> parameters deterministic-med
show protocols bgp <номер_AC> parameters
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      parameters {
         deterministic-med
      }
   }
}
```

Параметры

номер_AC

Номер AC в которой находится данный маршрутизатор. Значение должно лежать в диапазоне от 1 до 4294967296.

Значение по умолчанию

Отсутствует (детерминированный MED не внедряется).

Указания по использованию

Включение данной команды снимает временную зависимость от решений выбора оптимального пути на базе MED. Это гарантирует точное сравнение MED для всех маршрутов, полученных из одной и той же автономной системы. Если внедрение детерминированного MED отключено, то порядок получения маршрутов может повлиять на решения выбора оптимального пути на базе MED. Данная ситуация происходит, при получении одного и того же маршрута с одинаковой длиной пути, но разным значением атрибута MED от нескольких AC.

Форма **set** данной команды применяется для включения внедрения детерминированного MED.

Форма **delete** данной команды используется для отключения внедрения детерминированного MED.

Форма **show** данной команды используется для отображения текущей конфигурации в данном контексте.

28.7.15 protocols bgp <номер_AC> parameters distance global

Указание глобальной административной дистанции для всех маршрутов BGP.

Синтаксис

```
set protocols bgp <номер_AC> parameters distance global [external <дистанция> | internal <дистанция> | local <дистанция>]

delete protocols bgp <номер_AC> parameters distance global [external | internal | local]

show protocols bgp <номер_AC> parameters distance global
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      parameters {
         distance
            global
               external дистанция
               internal дистанция
               local дистанция
            }
         }
      }
   }
```

Параметры

номер_AC

Номер AC в которой находится данный маршрутизатор. Значение должно лежать в диапазоне от 1 до 4294967296.

external *дистанция*

Указание значения административной дистанции для внешних (eBGP) маршрутов. Значение должно лежать в диапазоне от 1 до 255.

internal *дистанция*

Указание значения административной дистанции для внутренних (iBGP) маршрутов. Значение должно лежать в диапазоне от 1 до 255.

local *дистанция*

Указание значения административной дистанции для внутренних локальных маршрутов. Значение должно лежать в диапазоне от 1 до 255.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения административной дистанции для маршрутов BGP. Значение всех трёх параметров (external, internal и local) должно быть определено.

Форма **set** данной команды применяется для указания глобальной административной дистанции маршрутов BGP.

Форма **delete** данной команды используется для удаления настройки глобальной административной дистанции маршрутов BGP.

Форма **show** данной команды используется для отображения текущей конфигурации в данном контексте.

28.7.16 protocols bgp <номер_AC> parameters distance prefix <подсеть> distance <дистанция>

Указание административной дистанции для маршрутов BGP для указанного префикса назначения.

Синтаксис

```
set protocols bgp <номер_AC> parameters distance prefix <подсеть> distance <дистанция>
delete protocols bgp <номер_AC> parameters distance prefix <подсеть>
show protocols bgp <номер_AC> parameters distance prefix <подсеть>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      parameters {
         distance {
            prefix подсеть {
               distance дистанция
            }
         }
      }
   }
}
```

Параметры

номер_AC

Номер AC в которой находится данный маршрутизатор. Значение должно лежать в диапазоне от 1 до 4294967296.

подсеть

Множественный узел. Используется формат ip-адрес/префикс. Возможно указание нескольких префиксов посредством создания соответствующего количества узлов конфигурации prefix.

дистанция

Значение административной дистанции для указанного префикса. Значение должно лежать в диапазоне от 1 до 255.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения административной дистанции для указанного префикса назначения.

Форма **set** данной команды применяется для указания административной дистанции.

Форма **delete** данной команды используется для удаления настройки административной дистанции для указанного префикса.

Форма **show** данной команды используется для отображения текущей конфигурации в данном контексте.

28.7.17 protocols bgp <номер_AC> parameters disable-network-import-check

Запрет проверки маршрутов IGP на наличие префикса в таблице маршрутизации.

Синтаксис

```
set protocols bgp <номер_AC> parameters disable-network-import-check
delete protocols bgp <номер_AC> parameters disable-network-import-check
show protocols bgp <номер_AC> parameters
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      parameters {
         disable-network-import-check
      }
   }
}
```

Параметры

номер_AC

Номер AC в которой находится данный маршрутизатор. Значение должно лежать в диапазоне от 1 до 4294967296.

Значение по умолчанию

Отсутствует (маршруты IGP проверяются на наличие префикса в таблице маршрутизации).

Указания по использованию

Эта команда используется для запрета проверки маршрутов IGP на наличие префикса в таблице маршрутизации. То есть при её применении, префикс будет анонсироваться несмотря на использование протокола IGP.

Форма **set** данной команды применяется для установки запрета проверки маршрутов IGP на наличие префикса в таблице маршрутизации.

Форма **delete** данной команды используется для снятия запрета проверки маршрутов IGP на наличие префикса в таблице маршрутизации.

Форма **show** данной команды используется для отображения текущей конфигурации в данном контексте.

28.7.18 protocols bgp <номер_AC> parameters enforce-first-as

Включение или отключение принудительной подстановки номеров AC в начало атрибута AS_PATH во всех входящих обновлениях для узлов eBGP.

Синтаксис

```
set protocols bgp <номер_AC> parameters enforce-first-as

delete protocols bgp <номер_AC> parameters enforce-first-as

show protocols bgp <номер_AC> parameters
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      parameters {
         enforce-first-as
      }
   }
}
```

Параметры

номер_AC

Номер AC в которой находится данный маршрутизатор. Значение должно лежать в диапазоне от 1 до 4294967296.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для включения или отключения принудительной подстановки номера AC в начало атрибута AS_PATH для узлов eBGP.

При включении данной команды, маршрутизатор будет отвергать обновления, полученные от узлов eBGP, если номер AC данного узла, не указан в начале атрибута AS_PATH. Данная опция применяется для предотвращения «спуффинга», когда неавторизованный или не правильно настроенный узел, изменяет направление трафика посредством объявления iBGP маршрута в качестве eBGP маршрута.

Форма **set** данной команды используется для включения

Форма **delete** данной команды используется для отключения

Форма **show** данной команды используется для отображения текущей конфигурации в данном контексте.

28.7.19 protocols bgp <номер_AC> parameters graceful-restart

Включение или отключение мягкого перезапуска процесса BGP.

Синтаксис

```
set protocols bgp <номер_AC> parameters graceful-restart [stalepath-time
<время>]

delete protocols bgp <номер_AC> parameters graceful-restart

show protocols bgp <номер_AC> parameters
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      parameters {
         graceful-restart {
            stalepath-time время
         }
      }
   }
}
```

Параметры

номер_AC

Номер AC в которой находится данный маршрутизатор. Значение должно лежать в диапазоне от 1 до 4294967296.

время

Максимальное значение интервала времени (в секундах), по истечении которого происходит удаление устаревших путей при перезагрузке узла. Значение должно лежать в диапазоне от 1 до 3600. По умолчанию установлено значение 360.

ПРИМЕЧАНИЕ Изменение значения данного параметра может повлечь за собой ухудшения работы сети.

Значение по умолчанию

Отсутствует (по умолчанию, при перезагрузке узла, устаревшие пути удаляются по истечению 360 секунд).

Указания по использованию

Эта команда применяется для включения или отключения мягкого перезапуска процесса BGP при перезагрузке маршрутизатора.

Форма **set** данной команды используется для включения мягкого перезапуска процесса BGP.

Форма **delete** данной команды используется для отключения мягкого перезапуска процесса BGP.

Форма **show** данной команды используется для отображения текущей конфигурации в данном контексте.

28.7.20 protocols bgp <номер_AC> parameters log-neighbor-changes

Включение журналирования изменения состояния соседних узлов BGP.

Синтаксис

```
set protocols bgp <номер_AC>c parameters log-neighbor-changes
delete protocols bgp <номер_AC> parameters log-neighbor-changes
show protocols bgp <номер_AC> parameters
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   bgp номер_AC {
      parameters {
         log-neighbor-changes
      }
```

```
    }
}
```

Параметры

номер_АС

Номер АС в которой находится данный маршрутизатор. Значение должно лежать в диапазоне от 1 до 4294967296.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда применяется для включения журналирования состояния соседних узлов BGP. При включении, отключении или перезапуске соседнего узла BGP запись об этом событии заносится в файл журнала. Данная команда может быть полезна для анализа проблем соединения.

Форма **set** данной команды используется для включения журналирования изменения состояния соседних узлов BGP.

Форма **delete** данной команды используется для отключения журналирования изменения состояния соседних узлов BGP.

Форма **show** данной команды используется для отображения текущей конфигурации в данном контексте.

28.7.21 protocols bgp <номер_АС> parameters no-fast-external-failover

Запрет автоматического перезапуска сессии BGP при разрыве соединения с соседним узлом BGP.

Синтаксис

```
set protocols bgp <номер_АС> parameters no-fast-external-failover
delete protocols bgp <номер_АС> parameters no-fast-external-failover
show protocols bgp <номер_АС> parameters
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    bgp номер_АС {
        parameters {
            no-fast-external-failover
        }
    }
}
```

Параметры

номер_АС

Номер АС в которой находится данный маршрутизатор. Значение должно лежать в диапазоне от 1 до 4294967296.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для установки запрета на автоматический перезапуск сессии BGP при разрыве соединения с соседним узлом BGP.

Форма **delete** данной команды используется для снятия запрета на автоматический перезапуск сессии BGP при разрыве соединения с соседним узлом BGP.

Форма **show** данной команды используется для отображения текущей конфигурации в данном контексте.

28.7.22 protocols bgp <номер_AC> parameters router-id <идентификатор>

Указание BGP ID для данного маршрутизатора.

Синтаксис

```
set protocols bgp <номер_AC> parameters router-id <идентификатор>
delete protocols bgp <номер_AC> parameters router-id <идентификатор>
show protocols bgp <номер_AC> parameters router-id
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols{
   bgp номер_AC {
      parameters {
         router-id идентификатор
      }
   }
}
```

Параметры

номер_AC

Номер AC в которой находится данный маршрутизатор. Значение должно лежать в диапазоне от 1 до 4294967296.

идентификатор

IPv4-адрес, используемый в качестве BGP ID.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания BGP ID для данного маршрутизатора. Если BGP ID не задан непосредственно с помощью этой команды, то в качестве BGP ID используется IP-адрес интерфейса заглушки. Если в системе отсутствуют определённые интерфейсы заглушки, то в качестве BGP ID будет использоваться первый IP-адрес, присвоенный физическому интерфейсу.

Форма **set** данной команды используется для указания BGP ID.

Форма **delete** данной команды используется для удаления заданного BGP ID и присвоения данному маршрутизатору BGP ID, созданного согласно правилам процесса выбора BGP ID.

Форма **show** данной команды используется для отображения текущей конфигурации в данном контексте.

28.7.23 protocols bgp <номер_AC> parameters scan-time <время>

Указание временного интервала между отправкой запроса на предоставление маршрутной информации по протоколу BGP.

Синтаксис

```
set protocols bgp <номер_AC> parameters scan-time <время>
delete protocols bgp <номер_AC> parameters scan-time <время>
show protocols bgp <номер_AC> parameters
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols{
   bgp номер_AC {
      parameters {
         scan-time время      }
   }
}
```

Параметры

номер_AC

Номер AC в которой находится данный маршрутизатор. Значение должно лежать в диапазоне от 1 до 4294967296.

время

Промежуток времени (в секундах), по истечению которого маршрутизатор отправляет запрос на получение маршрутной информации по протоколу BGP. Значение должно лежать в диапазоне от 5 до 60.

Значение по умолчанию

По умолчанию установлен временной интервал 15 секунд.

Указания по использованию

Форма **set** данной команды используется для указания временного интервала между отправкой запроса на предоставление маршрутной информации по протоколу BGP.

Форма **delete** данной команды используется для восстановления значения временного интервала, указанного по умолчанию.

Форма **show** данной команды используется для отображения текущей конфигурации в данном контексте.

28.7.24 clear ip bgp <адрес>

Сброс соединения BGP с указанным соседним узлом.

Синтаксис

```
clear ip bgp <адрес> [in [prefix-filter] | out | rsclient | soft [in | out]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

адрес

Сброс соединения с узлом BGP, имеющим указанный адрес IPv4 или IPv6.

in

Сброс входящих соединений BGP.

prefix-filter

Очистка списка фильтра исходящих маршрутов (Outbound route filter – ORF). ORF позволяет маршрутизаторам обмениваться информацией о настроенных фильтрах обновлений BGP. Данный параметр игнорируется до момента включения ORF в локальной системе. В противном случае происходит стандартный мягкий сброс.

out

Сброс исходящих соединений BGP.

rsclient

Сброс соединений, находящихся в информационной базе маршрутизации (RIB).

soft *in*

Сброс входящих соединений BGP без разрыва сессии.

soft *out*

Сброс исходящих соединений BGP без разрыва сессии

Значение по умолчанию

Производится сброс как входящих, так и исходящих соединений.

Указания по использованию

Команда позволяет осуществлять сброс соединения BGP с указанным соседним узлом. Применение новых политик BGP возможно только после осуществления сброса соединения. В последствии использовании данной команды происходит сброс соединений BGP, при этом сессия, установленная с указанным соседним узлом, переходит из состояния established в состояние idle, также производится очистка таблицы маршрутизации BGP. После сброса маршрутизатор заново получает всю маршрутную информацию от указанного соседнего узла, после чего производится формирование таблицы маршрутизации BGP на основании полученной информации.

При использовании параметра **soft** осуществляется сброс соединения BGP с указанным узлом без разрыва сессии. Таким образом, сохраняются маршруты, ранее полученные от указанного соседнего узла, версия таблицы (table version number) становится равной 0. При следующей отправке обновлений, маршрутизатор проверяет таблицу маршрутизации BGP и отправляет указанному соседнему узлу все маршруты, имеющие номер версии больше ноля. Таким образом осуществляется обновление политик BGP без разрыва соединения с соседним узлом.

28.7.25 clear ip bgp <адрес> ipv4 unicast

Сброс однонаправленного IPv4 соединения BGP.

Синтаксис

```
clear ip bgp <адрес> ipv4 unicast [in [prefix-filter] | out | soft [in | out]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

адрес

Сброс соединения с узлом BGP, имеющим указанный адрес IPv4 или IPv6.

in

Необязательный. Сброс входящих соединений BGP.

prefix-filter

Очистка списка фильтра исходящих маршрутов (Outbound route filter – ORF). ORF позволяет маршрутизаторам обмениваться информацией о настроенных фильтрах обновлений BGP. Данный параметр игнорируется до момента включения ORF в локальной системе. В противном

случае происходит стандартный мягкий сброс.

out

Сброс исходящих соединений BGP.

soft *in*

Сброс входящих соединений BGP без разрыва сессии.

soft *out*

Сброс исходящих соединений BGP без разрыва сессии

Значение по умолчанию

При отсутствии параметра **soft** производится сброс как входящих, так и исходящих соединений.

Указания по использованию

Команда позволяет осуществлять сброс однонаправленного IPv4 соединения BGP с указанным соседним узлом. Применение новых политик BGP возможно только после осуществления сброса соединения. В последствии использовании данной команды происходит сброс соединений BGP, при этом сессия, установленная с указанным соседним узлом, переходит из состояния established в состояние idle, также производится очистка таблицы маршрутизации BGP. После сброса маршрутизатор заново получает всю маршрутную информацию от указанного соседнего узла, после чего производится формирование таблицы маршрутизации BGP на основании полученной информации.

При использовании параметра **soft** осуществляется сброс соединения BGP с указанным узлом без разрыва сессии. Таким образом, сохраняются маршруты, ранее полученные от указанного соседнего узла, версия таблицы (table version number) становится равной 0. При следующей отправке обновлений, маршрутизатор проверяет таблицу маршрутизации BGP и отправляет указанному соседнему узлу все маршруты, имеющие номер версии больше ноля. Таким образом осуществляется обновление политик BGP без разрыва соединения с соседним узлом.

28.7.26 clear ip bgp dampening

Очистка информации о демпфировании колебаний маршрутов с восстановлением всех подавленных маршрутов.

Синтаксис

```
clear ip bgp dampening [<адрес> [<маска_подсети>] | <подсеть>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

адрес

Очистка информации о демпфировании колебаний маршрутов для узла с указанным адресом.

маска_подсети

Маска подсети IPv4-адреса, указанного в качестве значения параметра **ipv4-адрес**.

подсеть

Очистка информации о демпфировании колебаний маршрутов, для всех узлов, чьи адреса входя в указанную подсеть. Используется формат: *ip-адрес/префикс.*

Значение по умолчанию

При отсутствии дополнительных параметров, производится очистка информации о демпфировании колебаний маршрутов для всех узлов BGP. Кроме того, осуществляется восстановление всех подавленных маршрутов.

Указания по использованию

Данная команда используется для очистки информации, связанной с демпфированием колебаний маршрутов и для восстановления подавленных маршрутов.

28.7.27 routing bgp debug enable

Включение или отключения создания отладочного сообщения при возникновении события присвоения BGP ID, получения или отправки сообщения BGP.

Синтаксис

```
routing bgp debug enable
```

```
routing bgp debug disable
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для включения создания сообщений журналирования уровня *trace* при возникновении события присвоения BGP ID, отправке или получении сообщений BGP.

Форма **disable** данной команды используется для отключения создания сообщений журналирования уровня *trace* при возникновении события присвоения BGP ID, отправке или получении сообщений BGP.

28.7.28 routing bgp debug enable events

Включение или отключения создания отладочного сообщения при возникновении событий BGP.

Синтаксис

```
routing bgp debug enable events
```

```
routing bgp debug disable events
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для включения создания сообщений журналирования уровня *trace* при возникновении событий BGP.

Форма **disable** данной команды используется для отключения создания сообщений журналирования уровня *trace* при возникновении событий BGP.

28.7.29 routing bgp debug enable filters

Включение или отключения создания отладочного сообщения при возникновении событий, связанных с фильтрами BGP.

Синтаксис

```
routing bgp debug enable filters
```

```
routing bgp debug disable filters
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для включения создания сообщений журналирования уровня *trace* при возникновении событий, связанных с фильтрами BGP.

Форма **disable** данной команды используется для отключения отладки фильтров BGP.

28.7.30 routing bgp debug enable fsm

Включение или отключения создания отладочного сообщения при возникновении событий, связанных машиной конечных состояний (FSM) BGP.

Синтаксис

```
routing bgp debug enable fsm
routing bgp debug disable fsm
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для включения создания сообщений журналирования уровня *trace* при возникновении событий, связанных с фильтрами с машиной конечных состояний BGP.

Согласно спецификации RFC 1771, маршрутизатор BGP использует FSM с шестью фиксированными состояниями. Машина конечных состояний описывает порядок и последовательность принятия решений относительно реакции маршрутизатора на события, возникающие при соединении с соседними узлами BGP.

Форма **disable** данной команды используется для отключения отладки BGP FSM.

28.7.31 routing bgp debug enable keepalives

Включение или отключения создания отладочного сообщения при возникновении событий, связанных с отправкой и получением сообщений keep-alive.

Синтаксис

```
routing bgp debug enable keepalives
routing bgp debug disable keepalives
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для включения создания сообщений журналирования уровня *trace* при возникновении событий, связанных с отправкой и получением сообщений keep-alive.

Форма **disable** данной команды используется для отключения отладки сообщений keep-alive.

28.7.32 routing bgp debug enable updates

Отображение отладочной информации, связанной с обновлениями маршрутов BGP.

Синтаксис

```
routing bgp debug enable updates all | in | out
routing bgp debug disable updates
```

Режим интерфейса

Эксплуатационный режим.

Параметры

all

Отображение отладочной информации только для обновлений всех маршрутов.

in

Отображение отладочной информации только для обновлений входящих маршрутов.

out

Отображение отладочной информации только для обновлений исходящих маршрутов.

Значение по умолчанию

Отображается отладочная информация при возникновении события, связанного с обновлением как входящих, так и исходящих маршрутов.

Указания по использованию

Данная команда используется для включения создания сообщений журналирования уровня *trace* при возникновении событий, связанных с обновлением маршрутов BGP.

Форма **disable** данной команды используется для отключения отладки обновлений маршрутов BGP.

28.7.33 routing bgp debug enable zebra

Отображение отладочной информации, связанной с настройками демона Zebra BGP.

Синтаксис

```
routing bgp debug enable zebra
routing bgp debug disable zebra
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для включения создания сообщений журналирования уровня *trace* при возникновении событий, связанных с настройками демона Zebra BGP.

Форма **disable** данной команды используется для отключения отладки демона Zebra BGP.

28.7.34 routing bgp debug status

Отображение отладочных флагов протокола BGP.

Синтаксис

```
routing bgp debug status
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения отладочных флагов протокола BGP.

28.7.35 routing bgp debug disable

Отключение записи отладочной информации протокола BGP.

Синтаксис

```
routing bgp debug disable
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отключения создания отладочных сообщений, связанных с работой протокола BGP.

28.7.36 show ip bgp

Отображение маршрутов BGP.

Синтаксис

```
show ip bgp [<адрес> | <ipv4-подсеть> [longer-prefixes]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

адрес

Отображение маршрутов к соседнему узлу с указанным IPv4-адресом.

ipv4-подсеть

Отображение маршрутов к соседним узлам, находящимся в указанной IPv4-подсети.

longer-prefixes

Необязательный. Отображение списка всех маршрутов, полученных маршрутизатором для соседнего узла с указанным IPv4-адресом, либо для соседних узлов, находящихся в указанной IPv4-подсети.

Значение по умолчанию

Отображение всех маршрутов BGP.

Указания по использованию

Данная команда используется для отображения таблицы маршрутизации BGP.

28.7.37 show ip bgp attribute-info

Отображение информации об атрибутах сети BGP.

Синтаксис

```
show ip bgp attribute-info
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения информации об атрибутах сети BGP.

28.7.38 show ip bgp cidr-only

Отображение маршрутов BGP с бесклассовой адресацией.

Синтаксис

```
show ip bgp cidr-only
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения маршрутов BGP с бесклассовой адресацией.

28.7.39 show ip bgp community <сообщество>

Отображение маршрутов, принадлежащих определённым сообществам BGP.

Синтаксис

```
show ip bgp community <сообщество> exact-match
```

Режим интерфейса

Эксплуатационный режим.

Параметры

сообщество

Идентификатор сообщества BGP в формате AA:NN (где AA и NN должны лежать в диапазоне от 0 до 65535), либо идентификатор общепринятого сообщества BGP согласно спецификации RFC 1997 (local-AS, no-export и no-advertise). Возможно указание до четырёх идентификаторов сообществ, разделённых пробелом.

exact-match

Отображение только маршрутов, значение атрибута COMMUNITIES которых точно соответствует указанному сообществу.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения маршрутов, принадлежащих указанным сообществам.

28.7.40 show ip bgp community-info

Отображение информации о сообществе BGP.

Синтаксис

```
show ip bgp community-info
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения информации о сообществе BGP.

28.7.41 show ip bgp community-list <список_сообществ>

Отображение маршрутов, принадлежащих сообществам из определённого списка сообществ BGP.

Синтаксис

```
show ip bgp community-list <список_сообществ> [exact-match]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

список_сообществ

Определённый список сообществ BGP.

exact-match

Отображение только маршрутов, значение атрибута COMMUNITIES которых точно соответствует указанному сообществу.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения маршрутов BGP, принадлежащих сообществам из определённого списка сообществ BGP.

28.7.42 show ip bgp dampened-paths

Отображение текущего перечня подавленных маршрутов BGP.

Синтаксис

```
show ip bgp dampened-paths
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения текущего перечня подавленных маршрутов BGP.

28.7.43 show ip bgp filter-list <список_путей_ac>

Отображение маршрутов BGP, входящих в список путей AC.

Синтаксис

```
show ip bgp filter-list <список_путей_ac>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

список_путей_ac

Имя определённого списка путей AC.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения маршрутов BGP, входящих в список путей AC.

28.7.44 show ip bgp flap-statistics

Отображение статистики колебания маршрутов BGP.

Синтаксис

```
show ip bgp flap-statistics [<адрес> | <ipv4-подсеть> [longer-prefixes]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

адрес

Отображение статистики колебания маршрутов для маршрутов, соответствующих указанному IPv4-адресу.

ipv4-подсеть

Отображение статистики колебания маршрутов для маршрутов, соответствующих указанной IPv4-подсети.

longer-prefixes

Отображение только тех маршрутов из таблицы маршрутизации, у которых совпадает указанный префикс.

Значение по умолчанию

Отображение статистики колебаний маршрутов для всех маршрутов BGP.

Указания по использованию

Данная команда используется для отображения статистики колебаний маршрутов BGP.

28.7.45 show ip bgp flap-statistics cidr-only

Отображение статистики колебания маршрутов BGP для маршрутов с бесклассовой адресацией.

Синтаксис

```
show ip bgp flap-statistics cidr-only
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения статистики колебаний маршрутов BGP для маршрутов с бесклассовой адресацией.

28.7.46 show ip bgp flap-statistics filter-list <список_путей_ac>

Отображение статистики колебания маршрутов BGP для маршрутов, входящих в определённый список путей AC.

Синтаксис

```
show ip bgp flap-statistics filter-list список_путей_ac
```

Режим интерфейса

Эксплуатационный режим.

Параметры

список_путей_ac

Имя определённого списка путей AC.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения статистики колебаний маршрутов BGP для маршрутов, входящих в определённый список путей автономных систем.

28.7.47 show ip bgp flap-statistics prefix-list <список_префиксов>

Отображение статистики колебания маршрутов BGP для маршрутов с адресом, совпадающим с адресами из определённого списка префиксов.

Синтаксис

```
show ip bgp flap-statistics prefix-list <список_префиксов>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

список_префиксов

Имя определённого списка префиксов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения статистики колебания маршрутов BGP для маршрутов с адресом, совпадающим с адресами из определённого списка префиксов.

28.7.48 show ip bgp flap-statistics regexp <регулярное_выражение>

Отображение статистики колебания маршрутов BGP для маршрутов содержащих указанное регулярное выражение.

Синтаксис

show ip bgp flap-statistics regexp <регулярное_выражение>

Режим интерфейса

Эксплуатационный режим.

Параметры

регулярное_выражение

Регулярное выражение в формате POSIX, представляющее набор путей AC.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения статистики колебания маршрутов BGP для маршрутов содержащих указанное регулярное выражение.

28.7.49 show ip bgp flap-statistics route-map <имя_карты_маршрутов>

Отображение статистики колебания маршрутов BGP для маршрутов с адресом, входящим в определённую карту маршрутов.

Синтаксис

```
show ip bgp flap-statistics route-map <имя_карты_маршрутов>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_карты_маршрутов

Имя определённой карты маршрутов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения статистики колебания маршрутов BGP для маршрутов с адресом, входящим в определённую карту маршрутов.

28.7.50 show ip bgp ipv4 unicast

Отображение информации об однонаправленных IPv4-маршрутах.

Синтаксис

```
show ip bgp ipv4 unicast [<адрес> | <ipv4-подсеть> [longer-prefixes]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

адрес

Отображение информации BGP для указанного адреса.

ipv4-подсеть

Отображение информации BGP для указанной подсети.

longer-prefixes

Отображение только тех маршрутов из таблицы маршрутизации, у которых совпадает указанный префикс.

Значение по умолчанию

Отображение всех однонаправленных IPv4 маршрутов BGP.

Указания по использованию

Данная команда используется для отображения однонаправленных IPv4 маршрутов, находящихся в таблице маршрутизации BGP.

28.7.51 show ip bgp ipv4 unicast cidr-only

Отображение информации об однонаправленных IPv4-маршрутах.

Синтаксис

```
show ip bgp ipv4 unicast cidr-only
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсуствует.

Указания по использованию

Данная команда используется для отображения однонаправленных IPv4 маршрутов с бесклассовой адресацией.

28.7.52 show ip bgp ipv4 unicast community <сообщество>

Отображение однонаправленных IPv4-маршрутов BGP, принадлежащих определённому сообществу BGP.

Синтаксис

```
show ip bgp ipv4 unicast community <сообщество> [exact-match]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

сообщество

Идентификатор сообщества BGP в формате AA:NN (где AA и NN должны лежать в диапазоне от 0 до 65535), либо идентификатор общепринятого сообщества BGP согласно спецификации RFC 1997 (local-AS, no-export и no-advertise). Возможно указание до четырёх идентификаторов сообществ, разделённых пробелом.

exact-match

Отображение только маршрутов, значение атрибута COMMUNITIES которых точно соответствует указанному сообществу.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения однонаправленных IPv4-маршрутов, принадлежащих указанным сообществам.

28.7.53 show ip bgp ipv4 unicast community-list <список_сообществ>

Отображение однонаправленных IPv4-маршрутов, принадлежащих сообществам из определённого списка сообществ BGP.

Синтаксис

```
show ip bgp community-list <список_сообществ> [exact-match]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

список_сообществ

Определённый список сообществ BGP.

exact-match

Отображение только маршрутов, значение атрибута COMMUNITIES которых точно соответствует указанному сообществу.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения однонаправленных IPv4-маршрутов BGP, принадлежащих сообществам из определённого списка сообществ BGP.

28.7.54 show ip bgp ipv4 unicast filter-list <список_путей_ac>

Отображение однонаправленных IPv4-маршрутов BGP, входящих в список путей AC.

Синтаксис

```
show ip bgp ipv4 unicast filter-list список_путей_ac
```

Режим интерфейса

Эксплуатационный режим.

Параметры

список_путей_ac

Имя определённого списка путей AC.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения однонаправленных IPv4-маршрутов BGP, входящих в список путей AC.

28.7.55 show ip bgp ipv4 unicast neighbors

Отображение информации об однонаправленных IPv4-соединениях с соседними узлами BGP.

Синтаксис

```
show ip bgp ipv4 unicast neighbors
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения информации об однонаправленных IPv4-соединениях с соседними узлами BGP.

28.7.56 show ip bgp ipv4 unicast paths

Отображение информации об однонаправленных IPv4 путях BGP.

Синтаксис

```
show ip bgp ipv4 unicast paths
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения информации об однонаправленных IPv4 путях BGP.

28.7.57 show ip bgp ipv4 unicast prefix-list <список_префиксов>

Отображение перечня однонаправленных IPv4-маршрутов, адреса которых совпадают с адресами из определённого списка префиксов.

Синтаксис

```
show ip bgp ipv4 unicast prefix-list <список_префиксов>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

список_префиксов

Имя определённого списка префиксов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения однонаправленных IPv4-маршрутов, адреса которых совпадают с адресами из определённого списка префиксов.

28.7.58 show ip bgp ipv4 unicast regexp <регулярное_выражение>

Отображение однонаправленных IPv4-маршрутов BGP, содержащих указанное регулярное выражение.

Синтаксис

```
show ip bgp unicast regexp <регулярное_выражение>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

регулярное_выражение

Регулярное выражение в формате POSIX, представляющее набор путей AC.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения однонаправленных IPv4- маршрутов BGP, содержащих указанное регулярное выражение.

28.7.59 show ip bgp ipv4 unicast route-map <имя_карты_маршрутов>

Отображение однонаправленных IPv4-маршрутов BGP с адресами, входящими в определённую карту маршрутов.

Синтаксис

```
show ip bgp ipv4 unicast route-map <имя_карты_маршрутов>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_карты_маршрутов

Имя определённой карты маршрутов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения однонаправленных IPv4- маршрутов BGP с адресами, входящими в определённую карту маршрутов.

28.7.60 show ip bgp ipv4 unicast statistics

Отображение статистики для однонаправленных IPv4-маршрутов BGP.

Синтаксис

```
show ip bgp ipv4 unicast statistics
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения статистики для однонаправленных IPv4-маршрутов BGP.

28.7.61 show ip bgp ipv4 unicast summary

Отображение краткой информации об однонаправленных IPv4-маршрутов BGP.

Синтаксис

```
show ip bgp ipv4 unicast summary
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения краткой статистики для однонаправленных IPv4-маршрутов BGP.

28.7.62 show ip bgp neighbors

Отображение информации о соседних узлах BGP.

Синтаксис

```
show ip bgp neighbors
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения соседних узлов BGP.

28.7.63 show ip bgp memory

Отображение информации об объёме памяти, используемой процессом BGP.

Синтаксис

```
show ip bgp memory
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения информации об объёме памяти, используемой процессом BGP (в том числе память, используемую для размещения информационной базой маршрутизации (RIB), записей кэша, атрибутов, записей AS-PATH и результатов хеширования).

28.7.64 show ip bgp paths

Отображение путей BGP.

Синтаксис

```
show ip bgp paths
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения информации всех путей BGP.

28.7.65 show ip bgp prefix-list <список_префиксов>

Отображение перечня путей BGP, префиксы которых совпадают с префиксами из определённого списка префиксов.

Синтаксис

```
show ip bgp prefix-list <список_префиксов>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

список_префиксов

Имя определённого списка префиксов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения перечня путей BGP, префиксы которых совпадают с префиксами из определённого списка префиксов.

28.7.66 show ip bgp regexp <регулярное_выражение>

Отображение маршрутов BGP, содержащих указанное регулярное выражение.

Синтаксис

```
show ip bgp regexp <регулярное_выражение>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

регулярное_выражение

Регулярное выражение в формате POSIX, представляющее набор путей AC.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения маршрутов BGP, содержащих указанное регулярное выражение.

28.7.67 show ip bgp route-map <имя_карты_маршрутов>

Отображение маршрутов BGP, входящих в указанную карту маршрутов.

Синтаксис

```
show ip bgp route-map <имя_карты_маршрутов>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_карты_маршрутов

Имя определённой карты маршрутов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения маршрутов BGP, входящих в указанную карту маршрутов.

28.7.68 show ip bgp rsclient <адрес_узла>

Отображение маршрутов BGP, входящих в информационную базу маршрутизации.

Синтаксис

```
show ip bgp rsclient <адрес_узла> [summary]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

адрес_узла

IPv4-адрес соседнего узла BGP.

summary

Отображение краткой информации о маршрутах BGP, входящих в информационную базу маршрутизации.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения маршрутов BGP, входящих в информационную базу маршрутизации.

28.7.69 show ip bgp scan

Отображение статуса сети BGP.

Синтаксис

```
show ip bgp scan
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствую.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения статуса сети BGP.

28.7.70 show ip bgp summary

Отображение краткой информации о сети BGP.

Синтаксис

```
show ip bgp summary
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствую.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения краткой информации о сети BGP.

28.7.71 show ip route bgp

Отображение маршрутов BGP.

Синтаксис

```
show ip route bgp
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствую.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения маршрутов BGP.

28.7.72 show ipv6 bgp

Отображение маршрутов BGP.

Синтаксис

```
show ipv6 bgp [<ipv6-адрес> | <ipv6-подсеть> [longer-prefixes]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

ipv6-адрес

Отображение маршрутов к соседнему узлу с указанным IPv6-адресом.

ipv6-подсеть

Отображение маршрутов к соседним узлам, находящимся в указанной IPv6-подсети.

longer-prefixes

Отображение списка всех маршрутов, полученных маршрутизатором для соседнего узла с указанным IPv6-адресом, либо для соседних узлов, находящихся в указанной IPv6-подсети.

Значение по умолчанию

Отображение всех маршрутов BGP.

Указания по использованию

Данная команда используется для отображения таблицы маршрутизации BGP.

28.7.73 show ipv6 bgp community <сообщество>

Отображение маршрутов BGP, принадлежащих определённому сообществу BGP.

Синтаксис

```
show ipv6 bgp community <сообщество> [exact-match]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

сообщество

Идентификатор сообщества BGP в формате AA:NN (где AA и NN должны лежать в диапазоне от 0 до 65535), либо идентификатор общепринятого сообщества BGP согласно спецификации RFC 1997 (local-AS, no-export и no-advertise). Возможно указание до четырёх идентификаторов сообществ, разделённых пробелом.

exact-match

Отображение только маршрутов, значение атрибута COMMUNITIES которых точно соответствует указанному сообществу.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения маршрутов, принадлежащих указанным сообществам.

28.7.74 show ipv6 bgp community-list <список_сообществ>

Отображение маршрутов, принадлежащих сообществам из определённого списка сообществ BGP.

Синтаксис

```
show ipv6 bgp community-list <список_сообществ> [exact-match]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

список_сообществ

Определённый список сообществ BGP.

exact-match

Отображение только маршрутов, значение атрибута COMMUNITIES которых точно соответствует указанному сообществу.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения маршрутов BGP, принадлежащих сообществам из определённого списка сообществ BGP.

28.7.75 show ipv6 bgp filter-list <список_путей_ac>

Отображение маршрутов BGP, входящих в список путей AC.

Синтаксис

```
show ipv6 bgp filter-list <список_путей_ac>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

список_путей_ac

Имя определённого списка путей AC.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения маршрутов BGP, входящих в список путей AC.

28.7.76 show ipv6 bgp neighbor

Отображение информации о соседних узлах BGP.

Синтаксис

```
show ipv6 bgp neighbor
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения соседних узлов BGP.

28.7.77 show ipv6 bgp prefix-list <список_префиксов>

Отображение перечня путей BGP, префиксы которых совпадают с префиксами из определённого списка префиксов.

Синтаксис

```
show ipv6 bgp prefix-list <список_префиксов>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

список_префиксов

Имя определённого списка префиксов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения перечня путей BGP, префиксы которых совпадают с префиксами из определённого списка префиксов.

28.7.78 show ipv6 bgp regexp <регулярное_выражение>

Отображение маршрутов BGP, содержащих указанное регулярное выражение.

Синтаксис

```
show ipv6 bgp regexp <регулярное_выражение>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

регулярное_выражение

Регулярное выражение в формате POSIX, представляющее набор путей AC.

28.7.79 show ipv6 bgp summary

Отображение краткой информации о сети BGP.

Синтаксис

```
show ipv6 bgp summary
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствую.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения краткой информации о сети BGP.

29 Политики фильтрации маршрутов

29.1 Политики фильтрации маршрутов

Политика фильтрации маршрутов – это механизм, позволяющий настраивать критерии, с которыми будет сравниваться получаемая маршрутная информация, а в случае соответствия определенному критерию – выполнять для маршрута одно или несколько действий. Например, можно создать политику для фильтрации (блокирования) конкретных префиксов маршрутов, которые объявляются соседом по BGP. Кроме того, операторы политики используются для экспорта маршрутов, полученных по одному протоколу, например OSPF, в другой протокол, например BGP. Это обычно называется перераспределением маршрутов.

В настройке Numa edge политики фильтрации маршрутов сгруппированы под узлом policy, который служит контейнером для операторов политики; действующими операторами политики определяются правила, которые будут применяться к маршрутной информации.

Для ввода в действие уже определенной политики следует применить ее к конкретному протоколу маршрутизации. Политику можно применить либо в качестве политики импорта, либо в качестве политики экспорта к протоколам наподобие RIP, OSPF и BGP. В случае протокола BGP политики можно применять к каждому равноправному узлу в отдельности. К протоколу (или равноправному узлу BGP) можно применить только одну политику импорта и одну политику экспорта.

Политика, примененная к протоколу маршрутизации в качестве политики импорта, используется для обработки маршрутной информации, полученной по протоколу маршрутизации, к которому применяется политика. Например, если пользователь настроит политику импорта для протокола BGP, все объявления BGP, полученные системой Numa edge, будут вначале сравниваться с политикой импорта, после чего добавляться к таблицам BGP и таблицам маршрутизации.

Политика, примененная к протоколу маршрутизации в качестве политики экспорта, используется для обработки маршрутной информации, отправляемой по протоколу маршрутизации, к которому применяется политика. Например, если пользователь настраивает политику экспорта для BGP, то вся маршрутная информация BGP, исходящая из системы МЭ, будет сравниваться с оператором политики экспорта перед отправкой маршрутной информации любым равноправным узлам BGP.

Помимо контроля за маршрутной информацией, передаваемой по протоколу маршрутизации, политики экспорта используются также для обеспечения перераспределения маршрутов. Например, если пользователю нужно перераспределить полученные по OSPF маршруты на BGP, пользователь может настроить оператор политики, определяющий нужные ему маршруты OSPF, и затем применить этот оператор политики в качестве политики экспорта для OSPF.

29.1.1 Примеры настройки политик маршрутизации

В данном разделе приведены примеры настройки для политик маршрутизации. Здесь рассматриваются следующие вопросы:

- Фильтрация маршрутов с помощью списков доступа.
- Фильтрация входящих маршрутов с помощью списков префиксов.
- Фильтрация исходящих маршрутов с помощью списков путей автономных систем.

Фильтрация маршрутов с помощью списков доступа

В этом разделе рассматриваются следующие вопросы:

- Основная настройка RIP.
- Проверка настройки RIP.
- Создание политики фильтрации маршрутов.
- Применение политики фильтрации маршрутов.
- Проверка настройки политики фильтрации маршрутов.

Списки доступа можно использовать для фильтрации маршрутов для протоколов типа "расстояние-направление" наподобие RIP, а также на точках перераспределения в областях маршрутизации по состоянию канала (наподобие OSPF), где с их помощью можно контролировать, какие пути приходят в область или покидают её.

Ниже представлен пример настройки протокола RIP и политики фильтрации маршрутов. В первую очередь приводится настройка RIP, распределяющая все известные маршруты между тремя маршрутизаторами. Затем выполняется настройка политики фильтрации маршрутов с использованием списков доступа для высекания объявления одной сети. Пример настройки основан на эталонной схеме, приведенной на рис. 29.

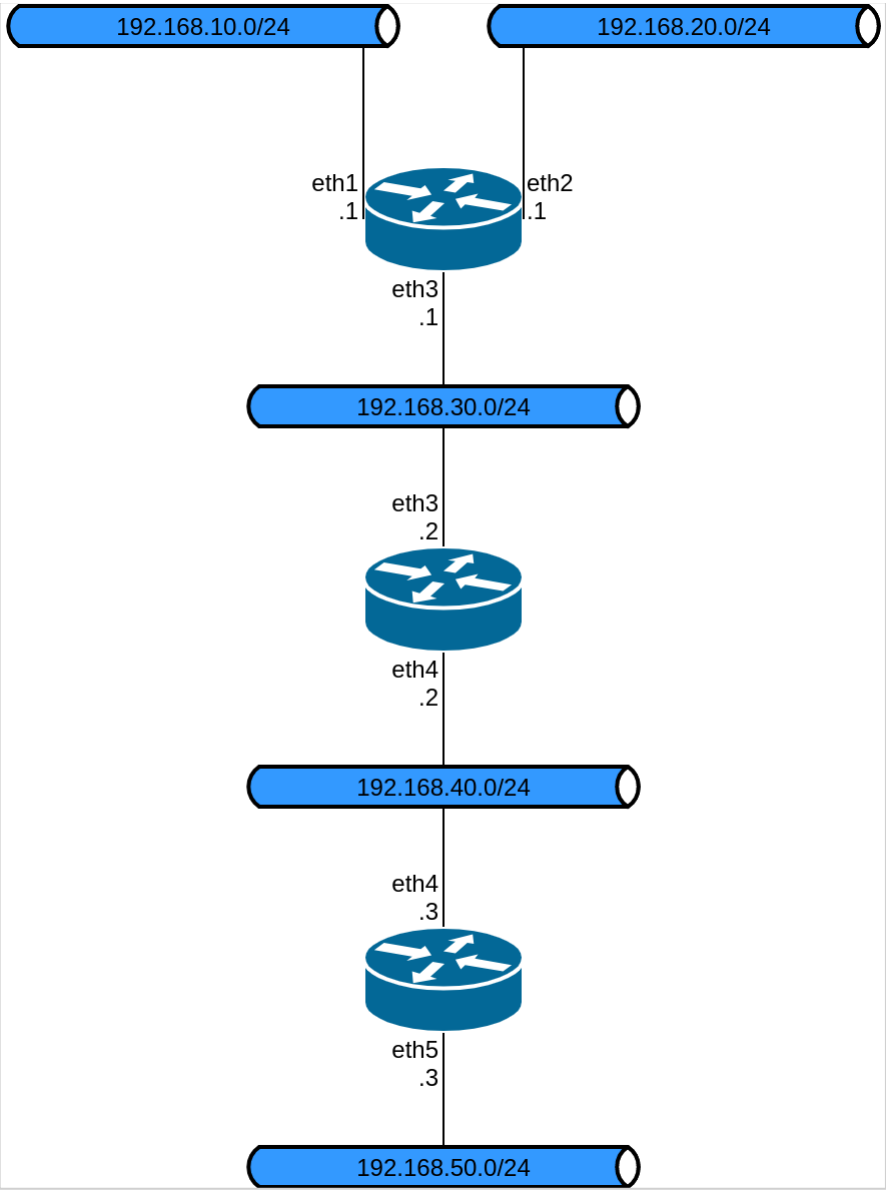


Рисунок 72 - Эталонная схема настройки RIP

Основная настройка RIP

В данном примере предполагается, что интерфейсы маршрутизатора уже настроены; настройка протокола RIP на каждом из маршрутизаторов приведена ниже.

Пример 279 - Основная настройка RIP

Маршрутизатор	Действие	Команда (команды)

Edge1	Отображение настройки.	[edit]
		admin@edge1# show protocols
		rip {
		network 192.168.30.0/24
		redistribute {
		connected {
		}
		}
		}

Маршрутизатор	Действие	Команда (команды)

Edge2	Отображение настройки.	[edit]
		admin@edge2# show protocols
		rip {
		network 192.168.30.0/24
		network 192.168.40.0/24
		redistribute {
		connected {
		}
		}
		}

Edge3	Отображение настройки.	[edit]
		admin@edge3# show protocols
		rip {
		network 192.168.40.0/24
		redistribute {
		connected {
		}
		}
		}

Проверка настройки RIP

Для проверки настройки RIP можно использовать следующие команды эксплуатационного режима.

Edge3: show ip route

В примере приведен вывод для команды **show ip route** для маршрутизатора Edge3.

Пример 280 - Проверка RIP на Edge3: "show ip route"

```
admin@edge3:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
       > - selected route, * - FIB route

C>* 127.0.0.0/8 is directly connected, lo
R>* 192.168.10.0/24 [120/3] via 192.168.40.2, eth4, 00:26:17
R>* 192.168.20.0/24 [120/3] via 192.168.40.2, eth4, 00:26:17
R>* 192.168.30.0/24 [120/2] via 192.168.40.2, eth4, 00:26:23
C>* 192.168.40.0/24 is directly connected, eth4
C>* 192.168.50.0/24 is directly connected, eth5
admin@edge3:~$
```

Из вывода видно, что маршруты к 192.168.10.0/24, 192.168.20.0/24 и 192.168.30.0/24 получены по RIP и что пакеты к этим сетям будут пересылаться наружу через eth4 на 192.168.40.2. Сети 192.168.40.0/24 и 192.168.50.0/24 подключены напрямую.

Edge3: show ip rip

В результате выполнения команды **show ip rip** для R3 отображаются аналогичные сведения, но в другом формате, что представлено в примере ниже.

Пример 281 - Проверка RIP на Edge3: “show ip rip”

```
admin@edge3:~$ show ip rip
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
      (n) - normal, (s) - static, (d) - default, (r) - redistribute,
      (i) - interface

     Network            Next Hop         Metric From            Tag Time
R(n) 192.168.10.0/24    192.168.40.2          3 192.168.40.2      0 02:55
R(n) 192.168.20.0/24    192.168.40.2          3 192.168.40.2      0 02:55
R(n) 192.168.30.0/24    192.168.40.2          2 192.168.40.2      0 02:55
C(i) 192.168.40.0/24    0.0.0.0               1 self              0
C(r) 192.168.50.0/24    0.0.0.0               1 self              0
admin@edge3:~$
```

Из вывода видно, что сети 192.168.10.0/24, 192.168.20.0/24 и 192.168.30.0/24 получены по RIP и что пакеты к этим сетям будут направлены на 192.168.40.2. Сети 192.168.40.0/24 и 192.168.50.0/24 подключены напрямую.

Создание политики фильтрации маршрутов

В этом разделе с помощью списков доступа выполняется настройка политики фильтрации маршрутов на Edge2 для отклонения входящих маршрутов от 10.0.20.0/24.

Пример 282 - Настройка фильтрации маршрутов

Маршрутизатор	Действие	Команда (команды)
Edge2	Создание списка доступа и правила для отклонения указанных маршрутов.	`[edit]` `admin@edge2# set policy access-list 100 rule 10 action deny`
	Соответствие любому получателю.	`[edit]` `admin@edge2# set policy access-list 100 rule 10 destination any`
	Соответствие отправителю 192.168.10.0	`[edit]` `admin@edge2# set policy access-list 100 rule 10 source network 192.168.10.0`
	Указание маски сети в дополнительном коде.	`[edit]` `admin@edge2# set policy access-list 100 rule 10 source inverse-mask 0.0.0.255`
	Создание правила для разрешения всех остальных маршрутов.	`[edit]` `admin@edge2# set policy access-list 100 rule 20 action permit`
	Соответствие любому получателю.	`[edit]` `admin@edge2# set policy access-list 100 rule 20 destination any`
	Соответствие любому отправителю.	`[edit]` `admin@edge2# set policy access-list 100 rule 20 source any`
	Фиксация изменений.	`[edit]` `admin@edge2# commit`

	Отображение настройки.	`[edit]`
		`admin@edge2# show policy`
		`  access-list 100 {`
		`  rule 10 {`
		`  action deny`
		`  destination {`
		`  any`
		`  }`
		`  source {`
		`  inverse-mask 0.0.0.255`

Маршрутизатор	Действие	Команда (команды)

		network 192.168.10.0
		}
		}
		rule 20 {
		action permit
		destination {
		any
		}
		source {
		any
		}
		}
		}

Применение политики фильтрации маршрутов

В этом разделе политика фильтрации маршрутов применяется ко входящим объявлениям RIP на Edge2.

Пример 283 - Применение политики фильтрации маршрутов

Маршрутизатор	Действие	Команда (команды)
Edge2	Использование списка доступа, созданного в предыдущем примере, для фильтрации входящих объявлений о маршрутах.	[edit] admin@edge2# set protocols rip distribute-list access-list in 100
	Фиксация настройки.	[edit] admin@edge2# commit

	Отображение настройки.	[edit]
		admin@edge2# show protocols
		rip {
		distribute-list {
		access-list {
		in 100
		}
		}
		network 192.168.30.0/24
		network 192.168.40.0/24
		redistribute {
		connected {
		}
		}
		}

Проверка настройки политики фильтрации маршрутов

Для проверки настройки политики фильтрации маршрутов можно использовать следующие команды эксплуатационного режима.

Edge3: show ip route

В примере ниже приведен вывод для команды **show ip route** для маршрутизатора Edge3.

Пример 284 - Проверка изменений политики фильтрации маршрутов на Edge3: ”show ip route”

```
admin@edge3:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
       > - selected route, * - FIB route

C>* 127.0.0.0/8 is directly connected, lo
R>* 192.168.20.0/24 [120/3] via 192.168.40.2, eth4, 00:25:12
R>* 192.168.30.0/24 [120/2] via 192.168.40.2, eth4, 00:25:13
C>* 192.168.40.0/24 is directly connected, eth4
C>* 192.168.50.0/24 is directly connected, eth5
```

Из вывода видно, что маршруты к 192.168.20.0/24 и 192.168.30.0/24 получены по RIP и что пакеты к этим сетям будут пересылаться наружу через eth4 на 192.168.40.2. Сети 192.168.40.0/24 и 192.168.50.0/24 подключены напрямую. Обратите внимание, что маршрута к 192.168.10.0/24 нет, так как он был отфильтрован политикой маршрутизации.

Edge3: show ip rip

В результате выполнения команды **show ip rip** для Edge3 отображаются аналогичные сведения, но в другом формате, что представлено в примере ниже.

Пример 285 - Проверка изменений политики фильтрации маршрутов на Edge3: ”show ip rip”

```
admin@edge3:~$ show ip rip
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
      (n) - normal, (s) - static, (d) - default, (r) - redistribute,
      (i) - interface

     Network            Next Hop         Metric From            Tag Time
R(n) 192.168.20.0/24    192.168.40.2          3 192.168.40.2      0 03:00
R(n) 192.168.30.0/24    192.168.40.2          2 192.168.40.2      0 03:00
C(i) 192.168.40.0/24    0.0.0.0               1 self              0
C(r) 192.168.50.0/24    0.0.0.0               1 self              0
```

Из вывода видно, что сети 192.168.20.0/24 и 192.168.30.0/24 получены по RIP и что пакеты к этим сетям будут направлены на 192.168.40.2. Сети 192.168.40.0/24 и 192.168.50.0/24 подключены напрямую. Отсутствует маршрут к 192.168.10.0/24.

Фильтрация входящих маршрутов с помощью списков префиксов

В данном разделе рассматриваются следующие вопросы:

- Настройка списка префиксов.
- Проверка входного фильтра.

Настройка списка префиксов

Обычным требованием к настройкам BGP является фильтрация входящих объявлений маршрутов от равноправного узла BGP. В системе Numa edge фильтрация такого рода выполняется при помощи политик фильтрации маршрутов, которые затем применяются к процессу BGP в качестве политик “импорта”. В данном примере для выполнения фильтрации применяются списки префиксов в сочетании с картами маршрутов.

В примере ниже создаются следующие политики фильтрации на входе:

- Edge1 должен принимать только сеть 192.168.200.0/24 от его равноправного узла eBGP и отклонять всё остальное.
- Edge4 должен разрешать все маршруты, но отклонять сеть 192.168.213.0/23, а также возможные подсети вплоть до /32.

Такая политика импорта показана на рисунке 86.

Принимается, что маршрутизаторы в AS64200 настроены для iBGP и eBGP как изображено, а также что маршрутизаторы в AS64201 и AS64202 настроены соответственно как равноправные узлы eBGP.

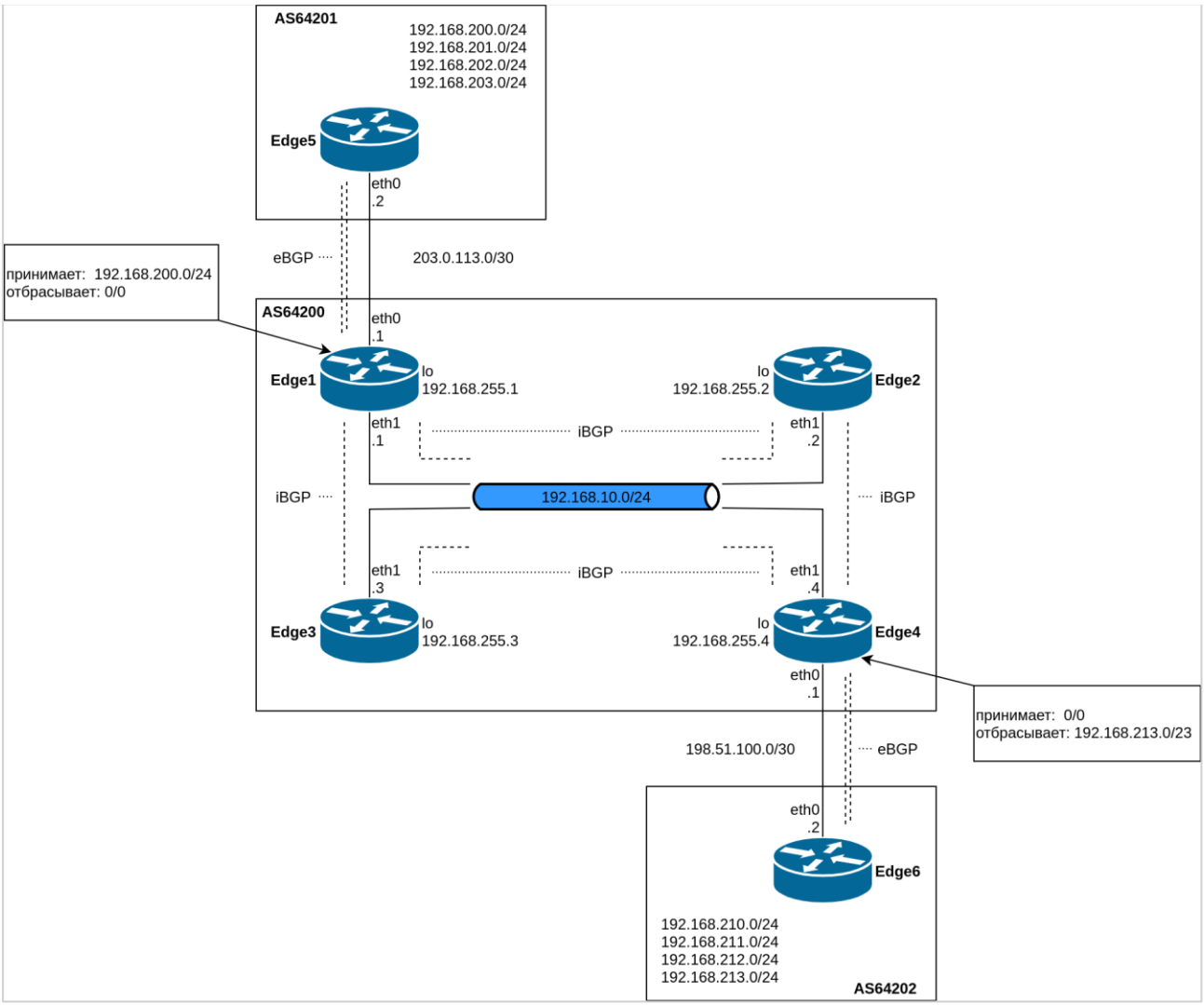


Рисунок 73- Фильтрация входящих маршрутов

Для создания фильтра входящих маршрутов следует выполнить следующие действия в режиме настройки:

Пример 286 - Создание политики импорта

Маршрутизатор	Действие	Команда (команды)
Edge1	Создание списка префиксов, которые следует разрешить. В данном случае такой префикс только один - 192.168.200.0/24.	[edit] admin@edge1# set policy prefix-list ALLOW-PREFIXES rule 10 action permit [edit] admin@edge1# set policy prefix-list ALLOW-PREFIXES rule 10 prefix 192.168.200.0/24
	Создание правила карты маршрутов для разрешения всех префиксов из списка.	[edit] admin@edge1# set policy route-map eBGP-IMPORT rule 10 action permit [edit] admin@edge1# set policy route-map eBGP-IMPORT rule 10 match ip address prefix-list ALLOW-PREFIXES
	Создание правила карты маршрутов для отклонения всех остальных префиксов.	[edit] admin@edge1# set policy route-map eBGP-IMPORT rule 20 action deny
	Назначение созданной политики карты	[edit]

Маршрутизатор	Действие	Команда (команды)
	маршрутов политикой карты маршрутов импорта для AS64201.	admin@edge1# set protocols bgp 64200 neighbor 203.0.113.2 route-map import eBGP-IMPORT
	Фиксация настройки.	[edit] admin@edge1# commit
	Сброс сеанса BGP с равноправным узлом для включения новых политик.	[edit] admin@edge1:~$ clear ip bgp 203.0.113.2

	Отображение настройки политики.	[edit]
		admin@edge1# show policy
		prefix-list ALLOW-PREFIXES {
		rule 10 {
		action permit
		prefix 192.168.200.0/24
		}
		}
		route-map eBGP-IMPORT {
		rule 10 {
		action permit
		match {
		ip {
		address {
		prefix-list ALLOW-PREFIXES
		}
		}
		}
		}
		rule 20 {
		action deny
		}
		}

	Отображение настройки BGP для соседа eBGP с адресом 203.0.113.2.	[edit]
		admin@edge1# show protocols bgp 64200 neighbor 203.0.113.2
		remote-as 64201
		route-map {
		import eBGP-IMPORT
		}

Edge4	Создание правила, которому будет соответствовать любой префикс от 192.168.213.0/23 до /26.	[edit] admin@edge4# set policy prefix-list DENY-RANGE-PREFIXES rule 10 action permit [edit] admin@edge4# set policy prefix-list DENY-RANGE-PREFIXES rule 10 le 26 [edit] admin@edge4# set policy prefix-list DENY-RANGE-PREFIXES rule 10 prefix 192.168.213.0/23
	Создание правила карты маршрутов для отклонения всех префиксов из списка.	[edit] admin@edge4# set policy route-map eBGP-IMPORT rule 10 action deny [edit] admin@edge4# set policy route-map eBGP-IMPORT rule 10 match ip address prefix-list DENY-RANGE-PREFIXES
	Создание правила карты маршрутов для разрешения всех остальных префиксов.	[edit] admin@edge4# set policy route-map eBGP-IMPORT rule 20 action permit

Маршрутизатор	Действие	Команда (команды)
	Назначение созданной политики карты маршрутов политикой карты маршрутов импорта для AS64202.	`[edit]` `admin@edge4# set protocols bgp 64200 neighbor 198.51.100.2 route-map import eBGP-IMPORT`
	Фиксация настройки.	`[edit]` `admin@edge4# commit`
	Сброс сеанса BGP с равноправным узлом для включения новых политик.	`[edit]` `admin@edge1:~$ clear ip bgp 198.51.100.2`

	Отображение настройки политики.	`[edit]`
		`admin@edge4# show policy`
		`prefix-list DENY-RANGE-PREFIXES {`
		`rule 10 {`
		`action permit le 26`
		`prefix 192.168.213.0/23`
		`}`
		`}`
		`route-map eBGP-IMPORT {`
		`rule 10 {`
		`action deny`
		`match {`
		`ip {`
		`address {`
		`prefix-list DENY-RANGE-PREFIXES`
		`}`
		`}`
		`}`
		`}`
		`rule 20 {`
		`action permit`
		`}`
		`}`

	Отображение настройки BGP для соседа eBGP с адресом 198.51.100.2.	`[edit]`
		`admin@edge4# show protocols bgp 64200 neighbor 198.51.100.2`
		`remote-as 64202`
		`route-map {`
		`import eBGP-IMPORT`
		`}`

Проверка входного фильтра

Для проверки настройки входного фильтра можно использовать следующие команды.

Edge1: show ip bgp (до применения фильтров)

В примере приведена таблица BGP маршрутизатора Edge1 перед применением фильтра импорта.

Пример 287 - Входящие маршруты BGP на Edge1 до фильтрации при импорте

```
admin@edge1:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.255.1
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
* i192.168.0.0      192.168.255.4            0    100      0 i
*>                  0.0.0.0                  0         32768 i
*> 192.168.200.0    203.0.113.2              0             0 64201 i
*> 192.168.201.0    203.0.113.2              0             0 64201 i
*> 192.168.202.0    203.0.113.2              0             0 64201 i
*> 192.168.203.0    203.0.113.2              0             0 64201 i
*>i192.168.210.0    198.51.100.2             0    100      0 64202 i
*>i192.168.211.0    198.51.100.2             0    100      0 64202 i
*>i192.168.212.0    198.51.100.2             0    100      0 64202 i
*>i192.168.213.0    198.51.100.2             0    100      0 64202 i

Displayed  9 out of 10 total prefixes
```

Edge1: show ip bgp (после применения фильтров)

В примере приведена таблица BGP маршрутизатора Edge1 после применения фильтров импорта.

Пример 288 - Входящие маршруты BGP на Edge1 после фильтрации при импорте

```
admin@edge1:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.255.1
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
* i192.168.0.0      192.168.255.4            0    100      0 i
*>                  0.0.0.0                  0         32768 i
*> 192.168.200.0    203.0.113.2              0             0 64201 i
*>i192.168.210.0    198.51.100.2             0    100      0 64202 i
*>i192.168.211.0    198.51.100.2             0    100      0 64202 i

Displayed  4 out of 5 total prefixes
```

Следует обратить внимание, что в таблице остался только элемент 192.168.200.0 от 203.0.113.2.

Edge4: show ip bgp

В примере приведена таблица BGP маршрутизатора Edge4 перед применением фильтров импорта.

Пример 289 - Входящие маршруты BGP на Edge4 до фильтрации при импорте

```
admin@edge4:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.255.4
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
* i192.168.0.0      192.168.255.1            0    100      0 i
*>                  0.0.0.0                  0         32768 i
*>i192.168.200.0    203.0.113.2              0    100      0 64201 i
*>i192.168.201.0    203.0.113.2              0    100      0 64201 i
*>i192.168.202.0    203.0.113.2              0    100      0 64201 i
*>i192.168.203.0    203.0.113.2              0    100      0 64201 i
*> 192.168.210.0    198.51.100.2             0             0 64202 i
*> 192.168.211.0    198.51.100.2             0             0 64202 i
*> 192.168.212.0    198.51.100.2             0             0 64202 i
*> 192.168.213.0    198.51.100.2             0             0 64202 i

Displayed  9 out of 10 total prefixes
```

Edge4: show ip bgp

Ниже приведена таблица BGP маршрутизатора Edge4 после применения фильтров импорта.

Пример 290 - Входящие маршруты BGP на Edge4 после фильтрации при импорте

```
admin@edge4:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.255.4
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
* i192.168.0.0      192.168.255.1            0    100      0 i
*>                  0.0.0.0                  0         32768 i
*>i192.168.200.0    203.0.113.2              0    100      0 64201 i
*> 192.168.210.0    198.51.100.2             0             0 64202 i
*> 192.168.211.0    198.51.100.2             0             0 64202 i

Displayed  4 out of 5 total prefixes
```

Следует обратить внимание, что под действие фильтра попали сети 192.168.212.0/24 и 192.168.213.0/24 от 198.51.100.2.

Фильтрация исходящих маршрутов с помощью списков путей автономных систем

В этом разделе рассматриваются следующие вопросы:

- Настройка AS-path-list.
- Проверка исходящего фильтра.

Настройка AS-path-list

Ещё одно обычное требование к настройке BGP – фильтрация исходящих префиксов. В системе Numa edge фильтрация такого рода выполняется при помощи политик фильтрации маршрутов, которые затем применяются к процессу BGP в качестве политик “экспорта”.

В примере, приведенном в данном разделе, предполагается, что системе AS64200 не нужно быть транзитной автономной системой для AS64201 или AS64202, что означает следующее:

- Маршруты eBGP от равноправного узла eBGP маршрутизатора Edge1 (AS64201) не следует отправлять на

равноправный узел eBGP маршрутизатора Edge4.

- Маршруты с равноправного узла eBGP маршрутизатора Edge4 (AS64202) не следует отправлять на равноправный узел eBGP маршрутизатора Edge1.

Если бы такая фильтрация *не была реализована*, то AS64203 мог бы отправлять трафик, предназначенный для AS64201, на маршрутизатор Edge4, и указанный трафик передавался бы через сеть AS64200.

В данном примере политикой экспорта BGP блокируется возможность AS64200 выступать в качестве транзитной сети для AS64201 и AS64202.

Описанная политика экспорта показана на рисунке ниже.

Принимается, что маршрутизаторы в AS64200 настроены для iBGP и eBGP как изображено и что маршрутизаторы в AS64201 и AS64202 настроены соответственно, как равноправные узлы eBGP (аналогично начальному положению примера настройки фильтрации по списку префиксов).

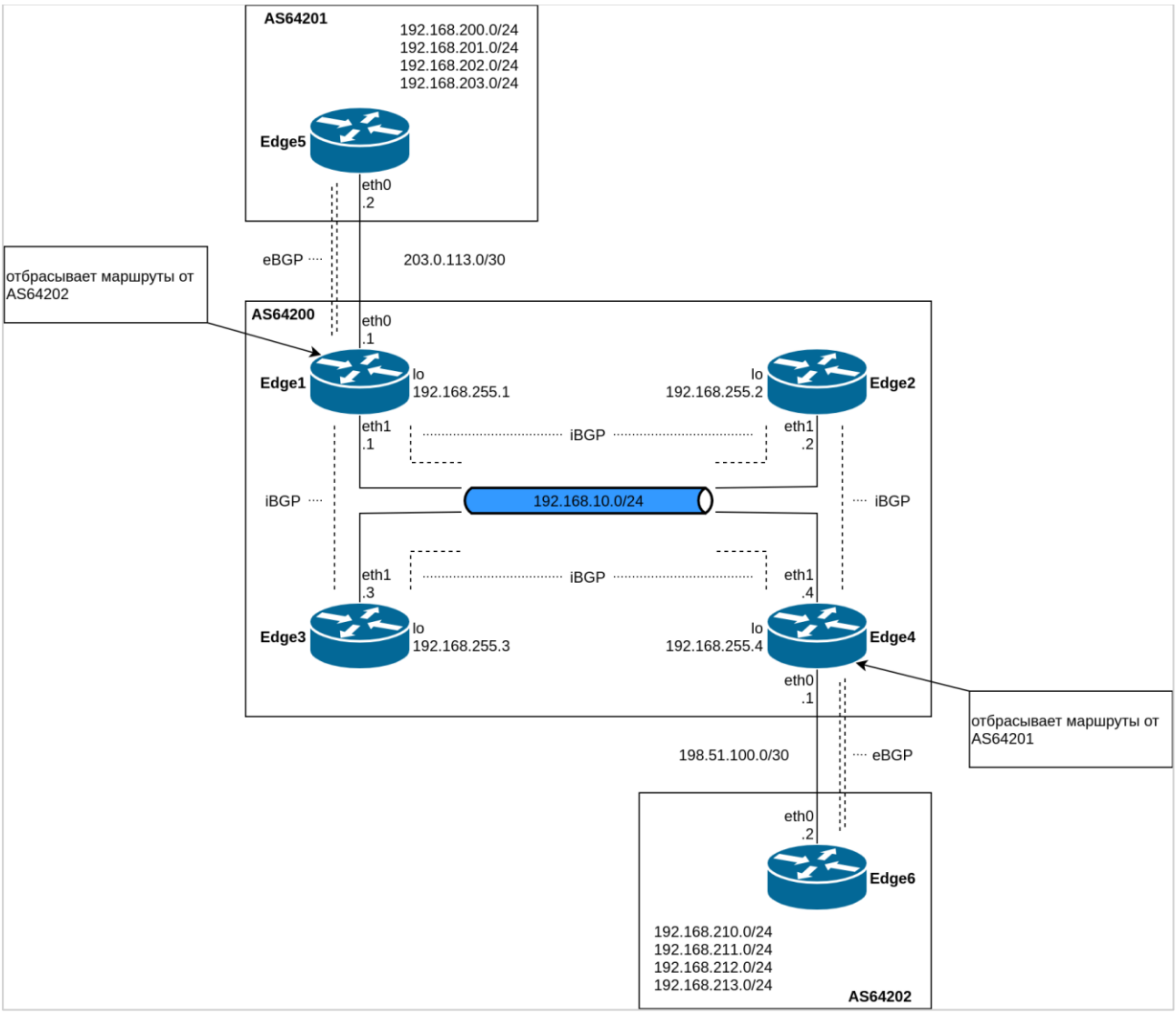


Рисунок 74- Фильтрация исходящих маршрутов

Для создания такой политики экспорта следует выполнить следующие действия в режиме настройки:

Пример 291 - Создание политики экспорта

Маршрутизатор	**Действие**	**Команда (команды)**

Edge1	Создание списка путей AS, которые следует отклонить. В данном случае такой только один - AS64202.	`[edit]`
		`admin@edge1# set policy as-path-list AS64202 rule 10 action permit`
		`[edit]`
		`admin@edge1# set policy as-path-list`

Маршрутизатор	Действие	Команда (команды)
		AS64202 rule 10 regex 64202
	Создание правила карты маршрутов для отклонения всех путей AS из списка.	[edit] admin@edge1# set policy route-map eBGP-EXPORT rule 10 action deny [edit] admin@edge1# set policy route-map eBGP-EXPORT rule 10 match as-path AS64202
	Создание правила карты маршрутов для разрешения всех остальных префиксов.	[edit] admin@edge1# set policy route-map eBGP-EXPORT rule 20 action permit
	Назначение созданной политики карты маршрутов политикой карты маршрутов экспорта для AS64201.	[edit] admin@edge1# set protocols bgp 64200 neighbor 203.0.113.2 route-map export eBGP-EXPORT
	Фиксация настройки.	[edit] admin@edge1# commit
	Сброс сеанса BGP с равноправным узлом для включения новых политик.	[edit] admin@edge1:~$ clear ip bgp 203.0.113.2

	Отображение настроек политик.	[edit]
		admin@edge1# show policy as-path-list AS64202 {
		rule 10 {
		action permit
		regex 64202
		}
		}
		route-map eBGP-EXPORT {
		rule 10 {
		action deny
		match {
		as-path AS64202
		}
		}
		rule 20 {
		action permit
		} }

	Отображение настройки BGP для соседа eBGP с адресом 203.0.113.2.	[edit]
		admin@edge1# show protocols bgp 64200 neighbor 203.0.113.2
		remote-as 200
		route-map {
		export eBGP-EXPORT
		}

Edge4	Создание списка путей AS, которые следует отклонить. В данном случае такая AS только одна - AS64201.	[edit] admin@edge4# set policy as-path-list AS64201 rule 10 action permit [edit] admin@edge4# set policy as-path-list AS64201 rule 10 regex 64201
	Создание правила карты маршрутов для отклонения всех путей AS из списка.	[edit] admin@edge4# set policy route-map eBGP-EXPORT rule 10 action deny [edit] admin@edge4# set policy route-map eBGP-EXPORT rule 10 match as-path AS64201
	Создание правила карты маршрутов для	[edit] admin@edge4# set policy route-map

Маршрутизатор	Действие	Команда (команды)
	разрешения всех остальных префиксов.	`eBGP-EXPORT rule 20 action permit`
	Назначение созданной политики карты маршрутов политикой карты маршрутов экспорта для AS 300.	`[edit]` `admin@edge4# set protocols bgp 64200 neighbor 198.51.100.2 route-map export eBGP-EXPORT`
	Фиксация настройки.	`[edit]` `admin@edge4# commit`
	Сброс сеанса BGP с равноправным узлом для включения новых политик.	`[edit]` `admin@edge4:~$ clear ip bgp 198.51.100.2`

	Отображение настроек политик.	`[edit]`
		`admin@edge4# show policy as-path-list AS64201 {`
		`rule 10 {`
		`action permit`
		`regex 64201`
		`}`
		`}`
		`route-map eBGP-EXPORT`
		`rule 10 {`
		`action deny`
		`match {`
		`as-path AS64201`
		`}`
		`}`
		`rule 20 {`
		`action permit`
		`} }`

	Отображение настройки BGP для соседа eBGP с адресом 99.99.99.2.	`[edit]`
		`admin@edge4# show protocols bgp 64200 neighbor 198.51.100.2`
		`remote-as 64202 route-map {`
		`export eBGP-EXPORT }`

Проверка исходящего фильтра

Для проверки настройки исходящего фильтра можно использовать следующие команды.

AS64201: show ip bgp

В примере приведена таблица BGP системы AS64201 *до* применения фильтров экспорта.

Пример 292 - Исходящие маршруты BGP на AS64201 до фильтрации при экспорте

```
admin@edge5:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.255.5
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.0.0      203.0.113.1              0             0 64200 i
*> 192.168.200.0    0.0.0.0                  0         32768 i
*> 192.168.201.0    0.0.0.0                  0         32768 i
*> 192.168.202.0    0.0.0.0                  0         32768 i
*> 192.168.203.0    0.0.0.0                  0         32768 i
*> 192.168.210.0    203.0.113.1                            0 64200 64202 i
*> 192.168.211.0    203.0.113.1                            0 64200 64202 i
*> 192.168.212.0    203.0.113.1                            0 64200 64202 i
*> 192.168.213.0    203.0.113.1                            0 64200 64202 i

Displayed  9 out of 9 total prefixes
```

AS64201: show ip bgp

В примере приведена таблица BGP системы AS64201 *после* применения фильтров экспорта.

Пример 293 - Исходящие маршруты BGP на AS64201 после фильтрации при экспорте

```
admin@edge5:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.255.5
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.0.0      203.0.113.1              0             0 64200 i
*> 192.168.200.0    0.0.0.0                  0         32768 i
*> 192.168.201.0    0.0.0.0                  0         32768 i
*> 192.168.202.0    0.0.0.0                  0         32768 i
*> 192.168.203.0    0.0.0.0                  0         32768 i

Displayed  5 out of 5 total prefixes
```

AS64202: show ip bgp

В примере приведена таблица BGP системы AS64202 *до* применения фильтров экспорта.

Пример 294 - Исходящие маршруты BGP на AS64202 до фильтрации при экспорте

```
admin@edge6:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.255.6
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.0.0      198.51.100.1             0             0 64200 i
*> 192.168.200.0    198.51.100.1                           0 64200 64201 i
*> 192.168.201.0    198.51.100.1                           0 64200 64201 i
*> 192.168.202.0    198.51.100.1                           0 64200 64201 i
*> 192.168.203.0    198.51.100.1                           0 64200 64201 i
*> 192.168.210.0    0.0.0.0                  0         32768 i
*> 192.168.211.0    0.0.0.0                  0         32768 i
*> 192.168.212.0    0.0.0.0                  0         32768 i
*> 192.168.213.0    0.0.0.0                  0         32768 i

Displayed  9 out of 9 total prefixes
```

AS64202: show ip bgp

В примере приведена таблица BGP системы AS64202 *после* применения фильтров экспорта.

Пример 295 - Исходящие маршруты BGP на AS64202 после фильтрации при экспорте

```
admin@edge6:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.255.6
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.0.0      198.51.100.1             0             0 64200 i
*> 192.168.210.0    0.0.0.0                  0         32768 i
*> 192.168.211.0    0.0.0.0                  0         32768 i
*> 192.168.212.0    0.0.0.0                  0         32768 i
*> 192.168.213.0    0.0.0.0                  0         32768 i

Displayed  5 out of 5 total prefixes
```

29.2 Команды политик фильтрации маршрутов

В данном разделе описаны команды политик фильтрации маршрутов системы Numa edge.

Команды настройки	
Списки доступа	
policy access-list <номер_списка>	Определение списка доступа.
policy access-list <номер_списка> description <описание>	Ввод краткого описания для списка доступа.
policy access-list <номер_списка> rule <номер_правила>	Создание правила для списка доступа.
policy access-list <номер_списка> rule <номер_правила> action <действие>	Указание действия, которое должно быть выполнено для пакетов, соответствующих правилу списка доступа.
policy access-list <номер_списка> rule <номер_правила> description <описание>	Ввод краткого описания для правила в списке доступа.
policy access-list <номер_списка> rule <номер_правила> destination <получатель>	Определение критерия соответствия в правиле списка доступа на основе получателя.

policy access-list <номер_списка> rule <номер_правила> source <отправитель>	Определение критериев соответствия для правила списка доступа на основе отправителя.
Списки доступа IPv6	
policy access-list6 <имя_списка>	Определение списка доступа IPv6.
policy access-list6 <имя_списка> description <описание>	Ввод краткого описания для списка доступа IPv6.
policy access-list6 <имя_списка> rule <номер_правила>	Создание правила для списка доступа IPv6.
policy access-list6 <имя_списка> rule <номер_правила> action <действие>	Указание действия, которое должно быть выполнено для пакетов, соответствующих правилу списка доступа IPv6.
policy access-list6 <имя_списка> rule <номер_правила> description <описание>	Ввод краткого описания для правила списка доступа IPv6.
policy access-list6 <имя_списка> rule <номер_правила> source <отправитель>	Определение критериев соответствия для правила списка доступа IPv6 на основе отправителя.
Списки путей AS	
policy as-path-list <имя_списка>	Определение списка путей автономных систем (AS).
policy as-path-list <имя_списка> description <описание>	Ввод краткого описания для списка путей AS.
policy as-path-list <имя_списка> rule <номер_правила>	Создание правила для списка путей AS.
policy as-path-list <имя_списка> rule <номер_правила> action <действие>	Указание действия, которое должно быть выполнено для пакетов, соответствующих правилу списка путей AS.
policy as-path-list <имя_списка> rule <номер_правила> description <описание>	Ввод краткого описания для правила списка путей AS.
policy as-path-list <имя_списка> rule <номер_правила> regex <regex>	Определение критериев соответствия для правила списка путей AS на основе регулярного выражения.
Списки сообщества	
policy community-list <номер_списка>	Определение списка сообщества BGP.
policy community-list <номер_списка> description <описание>	Ввод краткого описания для списка сообщества.
policy community-list <номер_списка> rule <номер_правила>	Создание правила для списка сообщества.
policy community-list <номер_списка> rule <номер_правила> action <действие>	Указание действия, которое должно быть выполнено для пакетов, соответствующих правилу списка сообщества.
policy community-list <номер_списка> rule <номер_правила> description <описание>	Ввод краткого описания для правила списка сообщества.
policy community-list <номер_списка> rule <номер_правила> regex <regex>	Определение критериев соответствия для правила списка путей сообщества на основе регулярного выражения.
Списки префиксов	
policy prefix-list <имя_списка>	Определение списка префиксов.
policy prefix-list <имя_списка> description <описание>	Ввод краткого описания для списка префиксов.
policy prefix-list <имя_списка> rule <номер_правила>	Создание правила для списка префиксов.
policy prefix-list <имя_списка> rule <номер_правила> action <действие>	Указание действия, которое должно быть выполнено для пакетов, соответствующих правилу списка префиксов.
policy prefix-list <имя_списка> rule <номер_правила> description <описание>	Ввод краткого описания для правила списка префиксов.
policy prefix-list <имя_списка> rule <номер_правила> ge <значение>	Определение критериев соответствия в правиле списка префиксов на основе численного сравнения со знаком "больше или равен".

policy prefix-list <имя_списка> rule <номер_правила> le <значение>	Определение критерия соответствия для правила списка префиксов на основе численного сравнения со знаком "меньше или равен".
policy prefix-list <имя_списка> rule <номер_правила> prefix <подсеть_ipv4>	Определение критериев соответствия для правила списка префиксов на основе подсети IPv4.
Списки префиксов IPv6	
policy prefix-list6 <имя_списка>	Определение списка префиксов IPv6.
policy prefix-list6 <имя_списка> description <описание>	Ввод краткого описания для списка префиксов IPv6.
policy prefix-list6 <имя_списка> rule <номер_правила>	Создание правила для списка префиксов IPv6.
policy prefix-list6 <имя_списка> rule <номер_правила> action <действие>	Указание действия, которое должно быть выполнено для пакетов, соответствующих правилу списка префиксов IPv6.
policy prefix-list6 <имя_списка> rule <номер_правила> description <описание>	Ввод краткого описания правила списка префиксов IPv6.
policy prefix-list6 <имя_списка> rule <номер_правила> ge <значение>	Определение критериев соответствия для правила списка префиксов IPv6 на основе численного сравнения со знаком "больше или равен".
policy prefix-list6 <имя_списка> rule <номер_правила> le <значение>	Определение критерия соответствия для правила списка префиксов IPv6 на основе численного сравнения со знаком "меньше или равен".
policy prefix-list6 <имя_списка> rule <номер_правила> prefix <подсеть_ipv6>	Определение критериев соответствия для правила списка префиксов на основе подсети IPv6.
Карты маршрутов	
policy route-map <имя_карты>	Определение карты маршрутов при маршрутизации на основе политик.
policy route-map <имя_карты> description <описание>	Ввод краткого описания для карты маршрутов.
policy route-map <имя_карты> rule <номер_правила>	Создание правила для карты маршрутов.
policy route-map <имя_карты> rule <номер_правила> action <действие>	Указание действия, которое должно быть выполнено для пакетов, соответствующих правилу карты маршрутов.
policy route-map <имя_карты> rule <номер_правила> call <имя_карты>	Вызов другой карты маршрутов.
policy route-map <имя_карты> rule <номер_правила> continue <номер_правила>	Вызов другого правила в текущей карте маршрутов.
policy route-map <имя_карты> rule <номер_правила> description <описание>	Ввод краткого описания для правила карты маршрутов.
policy route-map <имя_карты> rule <номер_правила> match as-path <имя_списка>	Определение условия соответствия для карты маршрутов на основе списка путей AS
policy route-map <имя_карты> rule <номер_правила> match community	Определение условия соответствия для карты маршрутов на основе сообществ BGP.
policy route-map <имя_карты> rule <номер_правила> match interface <интерфейс>	Определение условия соответствия для карты маршрутов на основе интерфейса первого транзитного узла.
policy route-map <имя_карты> rule <номер_правила> match ip address	Определение условия соответствия для карты маршрутов на основе IP-адреса.
policy route-map <имя_карты> rule <номер_правила> match ip nexthop	Определение условия соответствия для карты маршрутов на основе адреса следующего транзитного узла.
policy route-map <имя_карты> rule <номер_правила> match ip route-source	Определение условия соответствия для карты маршрутов на основе адреса, с которого объявляется маршрут.
policy route-map <имя_карты> rule <номер_правила> match ipv6 address	Определение условия соответствия для карты маршрутов на основе IPv6-адреса.

policy route-map <имя_карты> rule <номер_правила> match ipv6 nexthop	Определение условия соответствия для карты маршрутов на основе IPv6-адреса следующего транзитного узла.
policy route-map <имя_карты> rule <номер_правила> match metric <метрика>	Определение условия соответствия для карты маршрутов на основе метрики маршрута.
policy route-map <имя_карты> rule <номер_правила> match origin <способ_получения>	Определение условия соответствия для карты маршрутов на основе способа получения маршрута.
policy route-map <имя_карты> rule <номер_правила> match peer	Определение условия соответствия для карты маршрутов на основе IP-адреса равноправного узла.
policy route-map <имя_карты> rule <номер_правила> match tag <тег>	Определение условия соответствия для карты маршрутов на основе тега OSPF.
policy route-map <имя_карты> rule <номер_правила> on-match	Указание альтернативной политики выхода для карты маршрутов.
olicy route-map <имя_карты> rule <номер_правила> set aggregator	Изменение атрибута aggregator протокола BGP для маршрута.
policy route-map <имя_карты> rule <номер_правила> set as-path-prepend <добавляемая_строка>	Установка строки или ее добавление в начало пути AS для маршрута.
policy route-map <имя_карты> rule <номер_правила> set atomic-aggregate	Установка атрибута atomic-aggregate протокола BGP в маршруте.
policy route-map <имя_карты> rule <номер_правила> set comm-list	Изменение списка сообщества BGP в маршруте.
policy route-map <имя_карты> rule <номер_правила> set community	Изменение атрибута communities BGP в маршруте.
policy route-map <имя_карты> rule <номер_правила> set ip-next-hop <ipv4-адрес>	Изменение получателя следующего транзитного узла маршрута.
policy route-map <имя_карты> rule <номер_правила> set local-preference <local-pref>	Изменение атрибута local-pref BGP в маршруте.
policy route-map <имя_карты> rule <номер_правила> set metric <метрика>	Изменение метрики маршрута.
policy route-map <имя_карты> rule <номер_правила> set metric-type <тип>	Указание типа внешней метрики OSPF для маршрута.
policy route-map <имя_карты> rule <номер_правила> set origin <способ_получения>	Изменение кода BGP способа получения маршрута.
policy route-map <имя_карты> rule <номер_правила> set originator-id <ipv4-адрес>	Изменение атрибута идентификатора отправителя BGP для маршрута.
policy route-map <имя_карты> rule <номер_правила> set tag <тег>	Изменение значения тега OSPF маршрута.
policy route-map <имя_карты> rule <номер_правила> set weight <вес>	Изменение веса BGP маршрута.
Эксплуатационные команды	
policy show access-list	Отображение информации о списках доступа IPv4.
policy show access-list6	Отображение информации о списках доступа IPv6.
policy show as-path-list	Отображение информации о путевых списках AS.
policy show community-list	Отображение информации о списков сообществ.
policy show prefix-list	Отображение информации о списках префиксов IPv4.
policy show prefix-list6	Отображение информации о списках префиксов IPv6
show ip protocol	Отображение карт маршрутов IP по протоколам.
policy show route-map	Отображение сведений карты маршрутов.

29.2.1 policy access-list <номер_списка>

Определение списка доступа.

Синтаксис

```
set policy access-list <номер_списка>
delete policy access-list <номер_списка>
show policy access-list <номер_списка>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   access-list номер_списка {
   }
}
```

Параметры

номер_списка

Множественный узел. Численный идентификатор списка доступа. Допустимые значения представлены в таблице ниже:

Таблица 214 – Номера списков доступа

Значение	Описание
<1-99>	Стандартный список доступа IPv4
<100-199>	Расширенный список доступа IPv4
<1300-1999>	Стандартный список доступа IPv4 (расширенный диапазон)
<2000-2699>	Расширенный список доступа IPv4 (расширенный диапазон)

Можно создать несколько списков доступа, создав несколько узлов конфигурации policy access-list.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания списка доступа.

Форма **delete** этой команды используется для удаления списка доступа.

Форма **show** этой команды используется для отображения настройки списков доступа.

29.2.2 policy access-list <номер_списка> description <описание>

Ввод краткого описания списка доступа.

Синтаксис

```
set policy access-list <номер_списка> description <описание>
delete policy access-list <номер_списка> description
show policy access-list <номер_списка> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   access-list номер_списка {
      description описание
```

```
    }
}
```

Параметры

номер_списка

Множественный узел. Численный идентификатор списка доступа.

описание

Краткое текстовое описание для списка доступа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания описания списка доступа.

Форма **delete** этой команды используется для удаления описания списка доступа.

Форма **show** этой команды используется для отображения описания списка доступа.

29.2.3 policy access-list <номер_списка> rule <номер_правила>

Создание правила списка доступа.

Синтаксис

```
set policy access-list <номер_списка> rule <номер_правила>
delete policy access-list <номер_списка> rule <номер_правила>
show policy access-list <номер_списка> rule <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    access-list номер_списка {
        rule номер_правила {
        }
    }
}
```

Параметры

номер_списка

Множественный узел. Численный идентификатор списка доступа.

номер_правила

Множественный узел. Численный идентификатор правила. Допустимые значения представлены в таблице ниже:

Таблица 215 – Допустимые номера правил

Значение	Описание
<1-65535>	Номер правила

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания правила списка доступа.

Форма **delete** этой команды используется для удаления правила списка доступа.

Форма **show** этой команды используется для отображения параметров настройки правила списка доступа.

29.2.4 policy access-list <номер_списка> rule <номер_правила> action <действие>

Указание действия, которое должно быть выполнено для пакетов, соответствующих правилу списка доступа.

Синтаксис

```
set policy access-list <номер_списка> rule <номер_правила> action <действие>
delete policy access-list <номер_списка> rule <номер_правила> action
show policy access-list <номер_списка> rule <номер_правила> action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   access-list номер_списка {
      rule номер правила {
         action действие
      }
   }
}
```

Параметры

номер_списка

Множественный узел. Численный идентификатор списка доступа.

номер_правила

Множественный узел. Численный идентификатор правила.

действие

Обязательный. Указать, какое действие выполнять для адресов, соответствующих правилу. Допустимые значения указаны в таблице ниже:

Таблица 216 – Возможные действия при соответствии правилу

Значение	Описание
deny	Пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений
permit	Пакеты, соответствующие данному правилу, передаются в дальнейшую обработку

Значение по умолчанию

Пакеты, соответствующие данному правилу, передаются в дальнейшую обработку.

Указания по использованию

Форма **set** этой команды используется для определения действия, выполняемого над пакетом, удовлетворяющим критериям соответствия в данном правиле.

Форма **delete** этой команды используется для восстановления действия по умолчанию над пакетами, удовлетворяющими критериям соответствия.

Форма **show** этой команды используется для отображения параметров действия данного правила.

29.2.5 policy access-list <номер_списка> rule <номер_правила> description <описание>

Ввод краткого описания для правила в списке доступа.

Синтаксис

```
set policy access-list <номер_списка> rule <номер_правила> description <описание>
delete policy access-list <номер_списка> rule <номер_правила> description
show policy access-list <номер_списка> rule <номер_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    access-list номер_списка {
        rule номер правила {
            description описание
            }
        }
    }
}
```

Параметры

номер_списка

Множественный узел. Численный идентификатор списка доступа.

номер_правила

Множественный узел. Численный идентификатор правила.

описание

Краткое текстовое описание для правила в списке доступа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания описания правила в списке доступа.

Форма **delete** этой команды используется для удаления описания правила в списке доступа.

Форма **show** этой команды используется для отображения описания правила в списке доступа.

29.2.6 policy access-list <номер_списка> rule <номер_правила> destination <получатель>

Определение критерия соответствия в правиле списка доступа на основе получателя.

Синтаксис

```
set policy access-list <номер_списка> rule <номер_правила> destination <получатель>
delete policy access-list <номер_списка> rule <номер_правила> destination
show policy access-list <номер_списка> rule <номер_правила> destination
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    access-list номер_списка {
```

```
        rule номер правила {
            destination {
                получатель
            }
        }
    }
}
```

Параметры

номер_списка

Множественный узел. Численный идентификатор списка доступа.

номер_правила

Множественный узел. Численный идентификатор правила.

получатель

Параметры адреса назначения. Допустимые значения указаны в таблице ниже:

Таблица 217 – Возможные параметры адреса назначения

Значение	Описание
any	Соответствие для пакетов, предназначенных любому получателю
host ipv4-адрес	Соответствие для пакетов, предназначенных указанному узлу IPv4
inverse-mask маска	Соответствие для пакетов, предназначенных для подсетей, попадающих в указанную инвертированную маску
network ipv4-подсеть	Соответствие для пакетов, предназначенных указанной подсети IPv4

В команде обязательно должен присутствовать ровно один параметр из списка any, host, inverse-mask и network.

Значение по умолчанию

Отсутствует.

Указания по использованию

Если не указано никаких критериев соответствия, то фильтрация пакетов по получателю происходить не будет; это значит, что разрешены пакеты для всех получателей.

Указать источник пакетов можно лишь для расширенных списков доступа (диапазоны 100-199 и 2000-2699).

Форма **set** этой команды используется для указания критериев соответствия по получателю в данном правиле списка доступа.

Форма **delete** этой команды используется для удаления настроенных критериев соответствия по получателю в данном правиле.

Форма **show** этой команды используется для отображения параметров настройки фильтрации пакетов по получателю с помощью правил списка доступа.

29.2.7 policy access-list <номер_списка> rule <номер_правила> source <отправитель>

Определение критериев соответствия в правиле списка доступа на основе отправителя.

Синтаксис

```
set policy access-list <номер_списка> rule <номер_правила> source
<отправитель>

delete policy access-list <номер_списка> rule <номер_правила> source

show policy access-list <номер_списка> rule <номер_правила> source
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   access-list номер_списка {
      rule номер правила {
         source {
            отправитель
         }
      }
   }
}
```

Параметры

номер_списка

Множественный узел. Численный идентификатор списка доступа.

номер_правила

Множественный узел. Численный идентификатор правила.

отправитель

Параметры адреса источника. Допустимые значения указаны в таблице ниже:

Таблица 218 – Возможные параметры адреса назначения

Значение	Описание
any	Соответствие для пакетов, приходящих от любого отправителя
host ipv4-адрес	Соответствие для пакетов, приходящих от указанного узла IPv4
inverse-mask маска	Соответствие для пакетов, приходящих от подсетей, попадающих в указанную инвертированную маску
network ipv4-подсеть	Соответствие для пакетов, приходящих от указанной подсети IPv4

В команде обязательно должен присутствовать ровно один параметр из списка any, host, inverse-mask и network.

Значение по умолчанию

Отсутствует.

Указания по использованию

Если не указано никаких критериев соответствия, то фильтрация пакетов по получателю происходить не будет; это значит, что разрешены пакеты ото всех отправителей.

Указать источник пакетов можно лишь для расширенных списков доступа (диапазоны 100-199 и 2000-2699).

Форма **set** этой команды используется для указания критериев соответствия по отправителю в данном правиле списка доступа.

Форма **delete** этой команды используется для удаления настроенных критериев соответствия по отправителю в данном правиле.

Форма **show** этой команды используется для отображения параметров настройки фильтрации пакетов по отправителю с помощью правил списка доступа.

29.2.8 policy access-list6 <имя_списка>

Определение списка доступа IPv6.

Синтаксис

```
set policy access-list6 <имя_списка>
delete policy access-list6 <имя_списка>
show policy access-list6 <имя_списка>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   access-list6 имя_списка {
   }
}
```

Параметры

имя_списка

Множественный узел. Имя списка доступа IPv6 в текстовом формате.

Значение по умолчанию

Отсутствует.

Указания по использованию

Можно создать несколько списков доступа, создав несколько узлов конфигурации policy access-list6.

Форма **set** этой команды используется для создания списка доступа.

Форма **delete** этой команды используется для удаления списка доступа.

Форма **show** этой команды используется для отображения настройки списков доступа.

29.2.9 policy access-list6 <имя_списка> description <описание>

Ввод краткого описания списка доступа IPv6.

Синтаксис

```
set policy access-list6 <имя_списка> description <описание>
delete policy access-list6 <имя_списка> description
show policy access-list6 <имя_списка> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   access-list6 имя_списка {
      description описание
   }
}
```

Параметры

имя_списка

Множественный узел. Имя списка доступа IPv6 в текстовом формате.

описание

Краткое текстовое описание для списка доступа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания описания списка доступа.

Форма **delete** этой команды используется для удаления описания списка доступа.

Форма **show** этой команды используется для отображения описания списка доступа.

29.2.10 policy access-list6 <имя_списка> rule <номер_правила>

Создание правила списка доступа IPv6.

Синтаксис

```
set policy access-list6 <имя_списка> rule <номер_правила>
delete policy access-list6 <имя_списка> rule <номер_правила>
show policy access-list6 <имя_списка> rule <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   access-list6 имя_списка {
      rule номер_правила {
      }
   }
}
```

Параметры

имя_списка

Множественный узел. Имя списка доступа IPv6 в текстовом формате.

номер_правила

Множественный узел. Численный идентификатор правила. Допустимые значения представлены в таблице ниже:

Таблица 219 – Допустимые номера правил

Значение	Описание
<1-65535>	Номер правила

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания правила списка доступа.

Форма **delete** этой команды используется для удаления правила списка доступа.

Форма **show** этой команды используется для отображения параметров настройки правила списка доступа.

29.2.11 policy access-list6 <имя_списка> rule <номер_правила> action <действие>

Указание действия, которое должно быть выполнено для пакетов, соответствующих правилу списка доступа IPv6.

Синтаксис

```
set policy access-list6 <имя_списка> rule <номер_правила> action <действие>
delete policy access-list6 <имя_списка> rule <номер_правила> action
```

```
show policy access-list6 <имя_списка> rule <номер_правила> action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   access-list6 имя_списка {
      rule номер_правила {
         action действие
      }
   }
}
```

Параметры

имя_списка

Множественный узел. Имя списка доступа IPv6 в текстовом формате.

номер_правила

Множественный узел. Численный идентификатор правила.

действие

Обязательный. Указать, какое действие выполнять для пакетов, соответствующих данному правилу. Допустимые значения указаны в таблице ниже:

Таблица 220 – Возможные действия при соответствии правилу

Значение	Описание
deny	Пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений
permit	Пакеты, соответствующие данному правилу, передаются в дальнейшую обработку

Значение по умолчанию

Пакеты, соответствующие данному правилу, передаются в дальнейшую обработку.

Указания по использованию

Форма **set** этой команды используется для определения действия, выполняемого над пакетом, удовлетворяющим критериям соответствия в данном правиле.

Форма **delete** этой команды используется для восстановления действия по умолчанию над пакетами, удовлетворяющими критериям соответствия.

Форма **show** этой команды используется для отображения параметров действия данного правила.

29.2.12 policy access-list6 <имя_списка> rule <номер_правила> description <описание>

Ввод краткого описания правила списка доступа IPv6.

Синтаксис

```
set policy access-list6 <имя_списка> rule <номер_правила> description
<описание>

delete policy access-list6 <имя_списка> rule <номер_правила> description

show policy access-list6 <имя_списка> rule <номер_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
```

```
    access-list6 имя_списка {
        rule номер_правила {
            description описание
        }
    }
}
```

Параметры

имя_списка

Множественный узел. Имя списка доступа IPv6 в текстовом формате.

номер_правила

Множественный узел. Численный идентификатор правила.

описание

Краткое текстовое описание правила списка доступа.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания описания правила списка доступа.

Форма **delete** этой команды используется для удаления описания правила списка доступа.

Форма **show** этой команды используется для отображения описания правила списка доступа.

29.2.13 policy access-list6 <имя_списка> rule <номер_правила> source <отправитель>

Определение критериев соответствия в правиле списка доступа IPv6 на основе отправителя.

Синтаксис

```
set policy access-list6 <имя_списка> rule <номер_правила> source <отправитель>
delete policy access-list6 <имя_списка> rule <номер_правила> source
show policy access-list6 <имя_списка> rule <номер_правила> source
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    access-list6 имя_списка {
        rule номер_правила {
            source {
                отправитель
            }
        }
    }
}
```

Параметры

имя_списка

Множественный узел. Имя списка доступа IPv6 в текстовом формате.

номер_правила

Множественный узел. Численный идентификатор правила.

отправитель

Параметры адреса источника. Допустимые значения указаны в таблице ниже:

Таблица 221 – Возможные параметры адреса назначения

Значение	Описание
any	Соответствие для пакетов, приходящих от любого отправителя
exact-match	Соответствие для пакетов, приходящих от одного из префиксов подсетей
network ipv6-подсеть	Соответствие для пакетов, приходящих от указанной подсети IPv6

В команде обязательно должен присутствовать ровно один параметр из списка any, exact-match и network.

Значение по умолчанию

Отсутствует.

Указания по использованию

Если не указано никаких критериев соответствия, то фильтрация пакетов по получателю происходить не будет; это значит, что разрешены пакеты ото всех отправителей.

Форма **set** этой команды используется для указания критериев соответствия по отправителю в данном правиле списка доступа.

Форма **delete** этой команды используется для удаления настроенных критериев соответствия по отправителю в данном правиле.

Форма **show** этой команды используется для отображения параметров настройки фильтрации пакетов по отправителю с помощью правил списка доступа.

29.2.14 policy as-path-list <имя_списка>

Определение списка путей автономных систем (AS).

Синтаксис

```
set policy as-path-list <имя_списка>
delete policy as-path-list <имя_списка>
show policy as-path-list <имя_списка>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   as-path-list текст {
   }
}
```

Параметры

имя_списка

Множественный узел. Текстовый идентификатор списка путей AS. Можно создать несколько списков путей AS, создав несколько узлов конфигурации policy as-path-list.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для определения списка путей автономных систем (AS), используемого в маршрутизации на основе политик.

Форма **delete** этой команды используется для удаления списка путей AS.

Форма **show** этой команды используется для отображения настройки списка путей AS.

29.2.15 policy as-path-list <имя_списка> description <описание>

Ввод краткого описания списка путей AS.

Синтаксис

```
set policy as-path-list <имя_списка> description <описание>
delete policy as-path-list <имя_списка> description
show policy as-path-list <имя_списка> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   as-path-list текст {
      description текст
   }
}
```

Параметры

имя_списка

Текстовый идентификатор списка путей AS.

описание

Краткое текстовое описание списка путей AS.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания описания списка путей AS.

Форма **delete** этой команды используется для удаления описания списка путей AS.

Форма **show** этой команды используется для отображения описания списка путей AS.

29.2.16 policy as-path-list <имя_списка> rule <номер_правила>

Создание правила списка путей AS.

Синтаксис

```
set policy as-path-list <имя_списка> rule <номер_правила>
delete policy as-path-list <имя_списка> rule <номер_правила>
show policy as-path-list <имя_списка> rule <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   as-path-list текст {
      rule номер_правила {
      }
   }
```

```
}
```

Параметры

имя_списка

Текстовый идентификатор списка путей AS.

номер_правила

Множественный узел. Численный идентификатор правила. Допустимые значения представлены в таблице ниже:

Таблица 222 – Допустимые номера правил

Значение	Описание
<1-65535>	Номер правила

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания правила списка путей AS.

Форма **delete** этой команды используется для удаления правила списка путей AS.

Форма **show** этой команды используется для отображения параметров настройки правила списка путей AS.

29.2.17 policy as-path-list <имя_списка> rule <номер_правила> action <действие>

Указание действия, которое должно быть выполнено над пакетами, соответствующими правилу списка путей AS.

Синтаксис

```
set policy as-path-list <имя_списка> rule <номер_правила> action <действие>
delete policy as-path-list <имя_списка> rule <номер_правила> action
show policy as-path-list <имя_списка> rule <номер_правила> action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   as-path-list текст {
      rule номер_правила {
         action {
            действие
         }
      }
   }
}
```

Параметры

имя_списка

Текстовый идентификатор списка путей AS.

номер_правила

Численный идентификатор правила.

действие

Обязательный. Указать, какое действие выполнять для пакетов, соответствующих данному правилу. Допустимые значения указаны в таблице ниже:

Таблица 223 – Возможные действия при соответствии правилу

Значение	Описание
deny	Пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений
permit	Пакеты, соответствующие данному правилу, передаются в дальнейшую обработку

Значение по умолчанию

Пакеты, соответствующие данному правилу, передаются в дальнейшую обработку.

Указания по использованию

Форма **set** этой команды используется для определения действия, выполняемого над пакетом, удовлетворяющим критериям соответствия в данном правиле.

Форма **delete** этой команды используется для восстановления действия по умолчанию над пакетами, удовлетворяющих критериям соответствия.

Форма **show** этой команды используется для отображения параметров действия в данном правиле.

29.2.18 policy as-path-list <имя_списка> rule <номер_правила> description <описание>

Ввод краткого описания правила списка путей AS.

Синтаксис

```
set policy as-path-list <имя_списка> rule <номер_правила> description <описание>

delete policy as-path-list <имя_списка> rule <номер_правила> description

show policy as-path-list <имя-списка> rule <номер_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   as-path-list текст {
      rule номер_правила {
         description описание
      }
   }
}
```

Параметры

имя_списка

Текстовый идентификатор списка путей AS.

номер_правила

Численный идентификатор правила.

описание

Краткое текстовое описание правила списка путей AS.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания описания правила списка путей AS.

Форма **delete** этой команды используется для удаления описания правила списка путей AS.

Форма **show** этой команды используется для отображения описания правила списка путей AS.

29.2.19 policy as-path-list <имя_списка> rule <номер_правила> regex <regex>

Определение критериев соответствия в правиле списка путей AS на основе регулярного выражения.

Синтаксис

```
set policy as-path-list <имя_списка> rule <номер_правила> regex <regex>
delete policy as-path-list <имя_списка> rule <номер_правила> regex
show policy as-path-list <имя_списка> rule <номер_правила> regex
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   as-path-list текст {
      rule номер_правила {
         regex regex
      }
   }
}
```

Параметры

имя_списка

Текстовый идентификатор списка путей AS.

номер_правила

Численный идентификатор правила.

regex

Регулярное выражение в стиле POSIX, представляющее список путей AS.

Значение по умолчанию

Если регулярное выражение не определено, считается, что все пакеты соответствуют правилу.

Указания по использованию

Пакеты проверяются по тому, соответствуют ли пути AS, перечисленные в пакете, регулярному выражению, определенному с помощью этой команды. В зависимости от действия, определенного для правила при помощи команды **policy as-path-list <имя_списка> rule <номер_правила> action**, соответствующие пакеты либо разрешаются, либо отклоняются.

Форма **set** этой команды используется для определения критериев соответствия, которые будут использоваться при определении политики пересылки на основе путей AS.

Форма **delete** этой команды используется для удаления элемента с регулярным выражением. Если регулярное выражение не определено, считается, что все пакеты соответствуют правилу.

Форма **show** этой команды используется для отображения элемента с регулярным выражением.

29.2.20 policy community-list <номер_списка>

Определение списка сообщества BGP.

Синтаксис

```
set policy community-list <номер_списка>
delete policy community-list <номер_списка>
```

```
show policy community-list <номер_списка>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    community-list номер_списка {
    }
}
```

Параметры

номер_списка

Множественный узел. Численный идентификатор списка сообщества. Допустимые значения представлены в таблице ниже:

Таблица 224 – Допустимые номера списков сообществ

Значение	Описание
<1-99>	Стандартные номера списков сообществ BGP
<100-500>	Расширенные номера списков сообществ BGP

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания списка сообщества BGP, используемого в маршрутизации на основе политик.

Форма **delete** этой команды используется для удаления списка сообщества.

Форма **show** этой команды используется для отображения настройки списка сообщества.

29.2.21 policy community-list <номер_списка> description <описание>

Ввод краткого описания списка сообщества.

Синтаксис

```
set policy community-list <номер_списка> description <описание>
delete policy community-list <номер_списка> description
show policy community-list <номер_списка> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    community-list номер_списка {
        description описание
    }
}
```

Параметры

номер_списка

Множественный узел. Численный идентификатор списка сообщества.

описание

Краткое текстовое описание списка сообщества.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания описания списка сообщества.

Форма **delete** этой команды используется для удаления описания списка сообщества.

Форма **show** этой команды используется для отображения описания списка сообщества.

29.2.22 policy community-list <номер_списка> rule <номер_правила>

Создание правила списка сообщества.

Синтаксис

```
set policy community-list <номер_списка> rule <номер_правила>
delete policy community-list <номер_списка> rule <номер_правила>
show policy community-list <номер_списка> rule <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   community-list номер_списка {
      rule номер_правила {
      }
   }
}
```

Параметры

номер_списка

Множественный узел. Численный идентификатор списка сообщества.

номер_правила

Множественный узел. Численный идентификатор правила. Допустимые значения представлены в таблице ниже:

Таблица 225 – Допустимые номера правил

Значение	Описание
<1-65535>	Номер правила

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания правила списка сообщества.

Форма **delete** этой команды используется для удаления правила списка сообщества.

Форма **show** этой команды используется для отображения параметров настройки правила списка сообщества.

29.2.23 policy community-list <номер_списка> rule <номер_правила> action <действие>

Указание действия, которое должно быть выполнено над пакетами, соответствующими правилу списка сообщества.

Синтаксис

```
set policy community-list <номер_списка> rule <номер_правила> action <действие>
delete policy community-list <номер_списка> rule <номер_правила> action
show policy community-list <номер_списка> rule <номер_правила> action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    community-list номер_списка {
        rule номер_правила {
            action действие
        }
    }
}
```

Параметры

номер_списка

Множественный узел. Численный идентификатор списка сообщества.

номер_правила

Множественный узел. Численный идентификатор правила.

действие

Обязательный. Указать, какое действие выполнять для пакетов, соответствующих данному правилу. Допустимые значения указаны в таблице ниже:

Таблица 226 – Возможные действия при соответствии правилу

Значение	Описание
deny	Пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений
permit	Пакеты, соответствующие данному правилу, передаются в дальнейшую обработку

Значение по умолчанию

Пакеты, соответствующие данному правилу, передаются в дальнейшую обработку.

Указания по использованию

Форма **set** этой команды используется для определения действия, выполняемого над пакетом, удовлетворяющим критериям соответствия в данном правиле.

Форма **delete** этой команды используется для восстановления действия по умолчанию над пакетами, удовлетворяющими критериям соответствия.

Форма **show** этой команды используется для отображения параметров действия данного правила.

29.2.24 policy community-list <номер_списка> rule <номер_правила> description <описание>

Ввод краткого описания правила списка сообщества.

Синтаксис

```
set policy community-list <номер_списка> rule <номер_правила> description <описание>
delete policy community-list <номер_списка> rule <номер_правила> description
show policy community-list <номер_списка> rule <номер_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   community-list номер_списка {
      rule номер_правила {
         description описание
      }
   }
}
```

Параметры

номер_списка

Множественный узел. Численный идентификатор списка сообщества.

номер_правила

Множественный узел. Численный идентификатор правила.

описание

Краткое текстовое описание списка сообщества.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания описания правила списка сообщества.

Форма **delete** этой команды используется для удаления описания правила списка сообщества.

Форма **show** этой команды используется для отображения описания правила списка сообщества.

29.2.25 policy community-list <номер_списка> rule <номер_правила> regex <regex>

Определение критериев соответствия правила списка путей сообщества на основе регулярного выражения.

Синтаксис

```
set policy community-list <номер_списка> rule <номер_правила> regex <regex>
delete policy community-list <номер_списка> rule <номер_правила> regex
show policy community-list <номер_списка> rule <номер_правила> regex
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   community-list номер_списка {
      rule номер_правила {
         regex regex
      }
   }
}
```

Параметры

номер_списка

Множественный узел. Численный идентификатор списка сообщества.

номер_правила

Множественный узел. Численный идентификатор правила.

regex

Регулярное выражение в стиле POSIX, представляющее список сообщества BGP.

Значение по умолчанию

Если регулярное выражение не определено, считается, что все пакеты соответствуют правилу.

Указания по использованию

Пакеты проверяются по тому, соответствуют ли сообщества, перечисленные в пакете, регулярному выражению, определенному с помощью этой команды. В зависимости от действия, определенного для правила при помощи команды *policy community-list номер_списка rule номер_правила action*, соответствующие пакеты либо разрешаются, либо отклоняются.

Форма **set** этой команды используется для определения критериев соответствия, которые будут использоваться при определении политики пересылки на основе сообщества BGP.

Форма **delete** этой команды используется для удаления элемента с регулярным выражением. Если регулярное выражение не определено, считается, что все пакеты соответствуют правилу.

Форма **show** этой команды используется для отображения элемента с регулярным выражением.

29.2.26 policy prefix-list <имя_списка>

Определение списка префиксов.

Синтаксис

```
set policy prefix-list <имя_списка>
delete policy prefix-list <имя_списка>
show policy prefix-list <имя_списка>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   prefix-list имя_списка {
   }
}
```

Параметры

имя_списка

Множественный узел. Текстовый идентификатор для списка префиксов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания списка префиксов, используемого в маршрутизации на основе политик.

Форма **delete** этой команды используется для удаления списка префиксов.

Форма **show** этой команды используется для отображения настройки списка префиксов.

29.2.27 policy prefix-list <имя_списка> description <описание>

Ввод краткого описания списка префиксов.

Синтаксис

```
set policy prefix-list <имя_списка> description <описание>
delete policy prefix-list <имя_списка> description
show policy prefix-list <имя_списка> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   prefix-list имя_списка {
      description описание
   }
}
```

Параметры

имя_списка

Множественный узел. Текстовый идентификатор для списка префиксов.

описание

Краткое текстовое описание для списка путей.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания описания списка путей.

Форма **delete** этой команды используется для удаления описания списка путей.

Форма **show** этой команды используется для отображения описания списка путей.

29.2.28 policy prefix-list <имя_списка> rule <номер_правила>

Создание правила списка префиксов.

Синтаксис

```
set policy prefix-list <имя_списка> rule <номер_правила>
delete policy prefix-list <имя_списка> rule <номер_правила>
show policy prefix-list <имя_списка> rule <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   prefix-list имя_списка {
      rule номер_правила {
      }
   }
}
```

Параметры

имя_списка

Множественный узел. Текстовый идентификатор для списка префиксов.

номер_правила

Множественный узел. Численный идентификатор правила. Допустимые значения представлены в таблице ниже:

Таблица 227 – Допустимые номера правил

Значение	Описание
<1-65535>	Номер правила

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания правила списка префиксов.

Форма **delete** этой команды используется для удаления правила списка префиксов.

Форма **show** этой команды используется для отображения параметров настройки правила списка префиксов.

29.2.29 policy prefix-list <имя_списка> rule <номер_правила> action <действие>

Указание действия, которое должно быть выполнено над пакетами, соответствующими правилу списка префиксов.

Синтаксис

```
set policy prefix-list <имя_списка> rule <номер_правила> action <действие>
delete policy prefix-list <имя_списка> rule <номер_правила> action
show policy prefix-list <имя_списка> rule <номер_правила> action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   prefix-list имя_списка {
      rule номер_правила {
         action действие
      }
   }
}
```

Параметры

имя_списка

Множественный узел. Текстовый идентификатор для списка префиксов.

номер_правила

Множественный узел. Численный идентификатор правила.

действие

Обязательный. Указать, какое действие выполнять для пакетов, соответствующих данному правилу. Допустимые значения указаны в таблице ниже:

Таблица 228 – Возможные действия при соответствии правилу

Значение	Описание
deny	Пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений
permit	Пакеты, соответствующие данному правилу, передаются в дальнейшую обработку

Значение по умолчанию

Пакеты, соответствующие данному правилу, передаются в дальнейшую обработку.

Указания по использованию

Форма **set** этой команды используется для определения действия, выполняемого над пакетом, удовлетворяющим критериям соответствия в данном правиле.

Форма **delete** этой команды используется для восстановления действия по умолчанию над пакетами, удовлетворяющими критериям соответствия.

Форма **show** этой команды используется для отображения параметров действия данного правила.

29.2.30 policy prefix-list <имя_списка> rule <номер_правила> description <описание>

Ввод краткого описания правила списка префиксов.

Синтаксис

```
set policy prefix-list <имя_списка> rule <номер_правила> description <описание>

delete policy prefix-list <имя_списка> rule <номер_правила> description

show policy prefix-list <имя_списка> rule <номер_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   prefix-list имя_списка {
      rule номер_правила {
         description описание
      }
   }
}
```

Параметры

имя_списка

Множественный узел. Текстовый идентификатор для списка префиксов.

номер_правила

Множественный узел. Численный идентификатор правила.

описание

Краткое текстовое описание правила списка префиксов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания описания правила списка префиксов.

Форма **delete** этой команды используется для удаления описания правила списка префиксов.

Форма **show** этой команды используется для отображения описания правила списка префиксов.

29.2.31 policy prefix-list <имя_списка> rule <номер_правила> ge <значение>

Определение критериев соответствия в правиле списка префиксов на основе численного сравнения со знаком "больше или равен".

Синтаксис

```
set policy prefix-list <имя_списка> rule <номер_правила> ge <значение>
delete policy prefix-list <имя_списка> rule <номер_правила> ge
show policy prefix-list <имя_списка> rule <номер_правила> ge
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   prefix-list имя_списка {
      rule номер_правила {
         ge значение
      }
   }
}
```

Параметры

имя_списка

Множественный узел. Текстовый идентификатор для списка префиксов.

номер_правила

Множественный узел. Численный идентификатор правила.

значение

Число, представляющее префикс подсети. Данному правилу будут соответствовать префиксы подсетей, большие указанного числа или равные ему. Допустимые значения представлены в таблице ниже:

Таблица 229 – Возможные значения для сравнения

Значение	Описание
<0-32>	Числовые значения для сравнения с префиксами подсетей входящих пакетов

В правиле списка префиксов указывается определенная подсеть с помощью атрибута prefix. Дополнительно возможно указание атрибутов ge и le (возможно использовать вместе в рамках одного правила).

Общая логика указания атрибутов описывается выражением prefix-value < ge-value <= le-value. Выделяются или ограничиваются определенные диапазоны подсетей, входящие в сеть с заданным префиксом.

- Атрибут ge определяет наибольшую подсеть в рамках указанного префикса (атрибутом prefix). В числовом значении (маски) это меньшее число. Таким образом определяется диапазон подсетей меньших или равных указанной.
- Атрибут le определяет наименьшую подсеть в рамках указанного префикса (атрибутом prefix). В числовом значении (маски) это большее число.Таким образом определяется диапазон подсетей больших или равных указанной.

Значение по умолчанию

Если префикс не указан, считается, что все префиксы подсетей соответствуют правилу.

Указания по использованию

Префикс подсети входящих пакетов сравнивается с указанным значением; если префикс больше указанного префикса или равен ему, то соответствие правилу считается найденным, и выполняется действие, указанное в данном правиле.

Форма **set** этой команды используется для указания префикса подсети при определении политики фильтрации маршрутов.

Форма **delete** этой команды используется для удаления указанного префикса.

Форма **show** этой команды используется для отображения значения, указанного как префикс 'ge'.

29.2.32 policy prefix-list <имя_списка> rule <номер_правила> le <значение>

Определение критерия соответствия в правиле списка префиксов на основе численного сравнения со знаком "меньше или равен".

Синтаксис

```
set policy prefix-list <имя_списка> rule <номер_правила> le <значение>
delete policy prefix-list <имя_списка> rule <номер_правила> le
show policy prefix-list <имя_списка> rule <номер_правила> le
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   prefix-list имя_списка {
      rule номер_правила {
         le значение
      }
   }
}
```

Параметры

имя_списка

Множественный узел. Текстовый идентификатор для списка префиксов.

номер_правила

Множественный узел. Численный идентификатор правила.

значение

Число, представляющее префикс подсети. Данному правилу будут соответствовать префиксы подсетей, меньшие указанного числа или равные ему. Допустимые значения представлены в таблице ниже:

Таблица 230 – Возможные значения для сравнения

Значение	Описание
<0-32>	Числовые значения для сравнения с префиксами подсетей входящих пакетов

В правиле списка префиксов указывается определенная подсеть с помощью атрибута prefix. Дополнительно возможно указание атрибутов ge и le (возможно использовать вместе в рамках одного правила).

Общая логика указания атрибутов описывается выражением prefix-value < ge-value <= le-value. Выделяются или ограничиваются определенные диапазоны подсетей, входящие в сеть с заданным префиксом.

- Атрибут ge определяет наибольшую подсеть в рамках указанного префикса (атрибутом prefix). В числовом значении (маски) это меньшее число. Таким образом определяется диапазон подсетей меньших или равных указанной.
- Атрибут le определяет наименьшую подсеть в рамках указанного префикса (атрибутом prefix). В числовом значении (маски) это большее число.Таким образом определяется диапазон подсетей больших или равных указанной.

Значение по умолчанию

Если префикс не указан, считается, что все префиксы подсетей соответствуют правилу.

Указания по использованию

Префикс подсети входящих пакетов сравнивается с указанным значением; если префикс меньше указанного префикса или равен ему, то соответствие правилу считается найденным, и выполняется действие, указанное в данном правиле.

Форма **set** этой команды используется для указания префикса подсети при определении политики фильтрации маршрутов.

Форма **delete** этой команды используется для удаления указанного префикса.

Форма **show** этой команды используется для отображения значения, указанного как префикс 'le'.

29.2.33 policy prefix-list <имя_списка> rule <номер_правила> prefix <подсеть_ipv4>

Определение критериев соответствия в правиле списка префиксов на основе подсети IPv4.

Синтаксис

```
set policy prefix-list <имя_списка> rule <номер_правила> prefix <подсеть_ipv4>
delete policy prefix-list <имя_списка> rule <номер_правила> prefix
show policy prefix-list <имя_списка> rule <номер_правила> prefix
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   prefix-list имя_списка {
      rule номер_правила {
         prefix подсеть_ipv4
      }
   }
}
```

Параметры

имя_списка

Множественный узел. Текстовый идентификатор для списка префиксов.

номер_правила

Множественный узел. Численный идентификатор правила.

подсеть_ipv4

Подсеть IPv4. Данному правилу будут соответствовать подсети, в точности совпадающие с данной. Допустимые значения указаны в таблице ниже:

Таблица 231 – Формат указания подсети IPv4

Значение	Описание
<x.x.x.x/x>	Сеть IPv4

В правиле списка префиксов указывается определенная подсеть с помощью атрибута prefix. Дополнительно возможно указание атрибутов ge и le (возможно использовать вместе в рамках одного правила).

Общая логика указания атрибутов описывается выражением prefix-value < ge-value <= le-value. Выделяются или ограничиваются определенные диапазоны подсетей, входящие в сеть с заданным префиксом.

- Атрибут ge определяет наибольшую подсеть в рамках указанного префикса (атрибутом prefix). В числовом значении (маски) это меньшее число. Таким образом определяется диапазон подсетей меньших или равных указанной.

- Атрибут le определяет наименьшую подсеть в рамках указанного префикса (атрибутом prefix). В числовом значении (маски) это большее число.Таким образом определяется диапазон подсетей больших или равных указанной.

Значение по умолчанию

Если подсеть не указана, считается, что все подсети соответствуют правилу.

Указания по использованию

Подсеть, указанная во входящих пакетах, сравнивается с данным значением; если подсеть в точности совпадает с подсетью, указанной в команде, то соответствие правилу считается найденным, и выполняется действие, указанное в данном правиле.

Форма **set** этой команды используется для указания подсети при определении политики фильтрации маршрутов.

Форма **delete** этой команды используется для удаления указанного префикса. Если префикс не указан, считается, что все префиксы подсетей соответствуют правилу.

Форма **show** этой команды используется для отображения значения.

29.2.34 policy prefix-list6 <имя_списка>

Определение списка префиксов IPv6.

Синтаксис

```
set policy prefix-list6 <имя_списка>
delete policy prefix-list6 <имя_списка>
show policy prefix-list6 <имя_списка>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   prefix-list6 имя_списка {
   }
}
```

Параметры

имя_списка

Множественный узел. Текстовый идентификатор для списка префиксов IPv6.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания списка префиксов, используемого в маршрутизации на основе политик.

Форма **delete** этой команды используется для удаления списка префиксов.

Форма **show** этой команды используется для отображения настройки списка префиксов.

29.2.35 policy prefix-list6 <имя_списка> description <описание>

Ввод краткого описания списка префиксов IPv6.

Синтаксис

```
set policy prefix-list6 <имя_списка> description <описание>
delete policy prefix-list6 <имя_списка> description
show policy prefix-list6 <имя_списка> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   prefix-list6 имя_списка {
      description описание
   }
}
```

Параметры

имя_списка

Множественный узел. Текстовый идентификатор для списка префиксов IPv6.

описание

Краткое текстовое описание для списка путей.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания описания списка путей.

Форма **delete** этой команды используется для удаления описания списка путей.

Форма **show** этой команды используется для отображения описания списка путей.

29.2.36 policy prefix-list6 <имя_списка> rule <номер_правила>

Создание правила списка префиксов IPv6.

Синтаксис

```
set policy prefix-list6 <имя_списка> rule <номер_правила>
delete policy prefix-list6 <имя_списка> rule <номер_правила>
show policy prefix-list6 <имя_списка> rule <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   prefix-list6 имя_списка {
      rule номер_правила {
      }
   }
}
```

Параметры

имя_списка

Множественный узел. Текстовый идентификатор для списка префиксов IPv6.

номер_правила

Множественный узел. Численный идентификатор правила. Допустимые значения представлены в таблице ниже:

Таблица 232 – Допустимые номера правил

Значение	Описание
<1-65535>	Номер правила

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания правила списка префиксов.

Форма **delete** этой команды используется для удаления правила списка префиксов.

Форма **show** этой команды используется для отображения параметров настройки правила списка префиксов.

29.2.37 policy prefix-list6 <имя_списка> rule <номер_правила> action <действие>

Указание действия, которое должно быть выполнено над пакетами, соответствующими правилу списка префиксов IPv6.

Синтаксис

```
set policy prefix-list6 <имя_списка> rule <номер_правила> action <действие>
delete policy prefix-list6 <имя_списка> rule <номер_правила> action
show policy prefix-list6 <имя_списка> rule <номер_правила> action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   prefix-list6 имя_списка {
      rule номер_правила {
         action действие
      }
   }
}
```

Параметры

имя_списка

Множественный узел. Текстовый идентификатор для списка префиксов IPv6.

номер_правила

Множественный узел. Численный идентификатор правила.

действие

Обязательный. Указать, какое действие выполнять для пакетов, соответствующих данному правилу. Допустимые значения указаны в таблице ниже:

Таблица 233 – Возможные действия при соответствии правилу

Значение	Описание
deny	Пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений
permit	Пакеты, соответствующие данному правилу, передаются в дальнейшую обработку

Значение по умолчанию

Пакеты, соответствующие данному правилу, передаются в дальнейшую обработку.

Указания по использованию

Форма **set** этой команды используется для определения действия, выполняемого над пакетом, удовлетворяющим критериям соответствия в данном правиле.

Форма **delete** этой команды используется для восстановления действия по умолчанию для пакетов, удовлетворяющих критериям соответствия.

Форма **show** этой команды используется для отображения параметров действия данного правила.

29.2.38 policy prefix-list6 <имя_списка> rule <номер_правила> description <описание>

Ввод краткого описания правила списка префиксов IPv6.

Синтаксис

```
set policy prefix-list6 <имя_списка> rule <номер_правила> description <описание>
delete policy prefix-list6 <имя_списка> rule <номер_правила> description
show policy prefix-list6 <имя_списка> rule <номер_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   prefix-list6 имя_списка {
      rule номер_правила {
         description описание
      }
   }
}
```

Параметры

имя_списка

Множественный узел. Текстовый идентификатор для списка префиксов IPv6.

номер_правила

Множественный узел. Численный идентификатор правила.

описание

Краткое текстовое описание правила списка префиксов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания описания правила списка префиксов.

Форма **delete** этой команды используется для удаления описания правила списка префиксов.

Форма **show** этой команды используется для отображения описания правила списка префиксов.

29.2.39 policy prefix-list6 <имя_списка> rule <номер_правила> ge <значение>

Определение критериев соответствия в правиле списка префиксов IPv6 на основе численного сравнения со знаком "больше или равен".

Синтаксис

```
set policy prefix-list6 <имя_списка> rule <номер_правила> ge <значение>
delete policy prefix-list6 <имя_списка> rule <номер_правила> ge
show policy prefix-list6 <имя_списка> rule <номер_правила> ge
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   prefix-list имя_списка {
      rule номер_правила {
         ge значение
      }
   }
}
```

Параметры

имя_списка

Множественный узел. Текстовый идентификатор для списка префиксов IPv6.

номер_правила

Множественный узел. Численный идентификатор правила.

значение

Число, представляющее префикс подсети IPv6. Данному правилу будут соответствовать префиксы подсетей, большие указанного числа или равные ему. Допустимые значения представлены в таблице ниже:

Таблица 234 – Возможные значения для сравнения

Значение	Описание
<0-128>	Числовые значения для сравнения с префиксами подсетей входящих пакетов

Общая логика указания атрибутов описывается выражением prefix-value < ge-value <= le-value. Выделяются или ограничиваются определенные диапазоны подсетей, входящие в сеть с заданным префиксом.

- Атрибут ge определяет наибольшую подсеть в рамках указанного префикса (атрибутом prefix). В числовом значении (маски) это меньшее число. Таким образом определяется диапазон подсетей меньших или равных указанной.
- Атрибут le определяет наименьшую подсеть в рамках указанного префикса (атрибутом prefix). В числовом значении (маски) это большее число.Таким образом определяется диапазон подсетей больших или равных указанной.

Значение по умолчанию

Если префикс не указан, считается, что все префиксы подсетей соответствуют правилу.

Указания по использованию

Префикс подсети входящих пакетов сравнивается с указанным значением; если префикс больше указанного префикса или равен ему, то соответствие правилу считается найденным, и выполняется действие, указанное в данном правиле.

Форма **set** этой команды используется для указания префикса подсети при определении политики фильтрации маршрутов.

Форма **delete** этой команды используется для удаления указанного префикса.

Форма **show** этой команды используется для отображения значения, указанного как префикс 'ge'.

29.2.40 policy prefix-list6 <имя_списка> rule <номер_правила> le <значение>

Определение критерия соответствия в правиле списка префиксов IPv6 на основе численного сравнения со знаком "меньше или равен".

Синтаксис

```
set policy prefix-list6 <имя_списка> rule <номер_правила> le <значение>
```

```
delete policy prefix-list6 <имя_списка> rule <номер_правила> le
show policy prefix-list6 <имя_списка> rule <номер_правила> le
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   prefix-list имя_списка {
      rule номер_правила {
         le значение
      }
   }
}
```

Параметры

имя_списка

Множественный узел. Текстовый идентификатор для списка префиксов IPv6.

номер_правила

Множественный узел. Численный идентификатор правила.

значение

Число, представляющее префикс подсети IPv6. Данному правилу будут соответствовать префиксы подсетей, меньшие указанного числа или равные ему. Допустимые значения представлены в таблице ниже:

Таблица 235 – Возможные значения для сравнения

Значение	Описание
<0-128>	Числовые значения для сравнения с префиксами подсетей входящих пакетов

В правиле списка префиксов указывается определенная подсеть с помощью атрибута prefix. Дополнительно возможно указание атрибутов ge и le (возможно использовать вместе в рамках одного правила).

Общая логика указания атрибутов описывается выражением prefix-value < ge-value <= le-value. Выделяются или ограничиваются определенные диапазоны подсетей, входящие в сеть с заданным префиксом.

- Атрибут ge определяет наибольшую подсеть в рамках указанного префикса (атрибутом prefix). В числовом значении (маски) это меньшее число. Таким образом определяется диапазон подсетей меньших или равных указанной.
- Атрибут le определяет наименьшую подсеть в рамках указанного префикса (атрибутом prefix). В числовом значении (маски) это большее число.Таким образом определяется диапазон подсетей больших или равных указанной.

Значение по умолчанию

Если префикс не указан, считается, что все префиксы подсетей соответствуют правилу.

Указания по использованию

Префикс подсети входящих пакетов сравнивается с указанным значением; если префикс меньше указанного префикса или равен ему, то соответствие правилу считается найденным, и выполняется действие, указанное в данном правиле.

Форма **set** этой команды используется для указания префикса подсети при определении политики фильтрации маршрутов.

Форма **delete** этой команды используется для удаления указанного префикса.

Форма **show** этой команды используется для отображения значения, указанного как префикс 'le'.

29.2.41 policy prefix-list6 <имя_списка> rule <номер_правила> prefix <подсеть_ipv6>

Определение критериев соответствия в правиле списка префиксов на основе подсети IPv6.

Синтаксис

```
set policy prefix-list6 <имя_списка> rule <номер_правила> prefix <подсеть_ipv6>
delete policy prefix-list6 <имя_списка> rule <номер_правила> prefix
show policy prefix-list6 <имя_списка> rule <номер_правила> prefix
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   prefix-list имя_списка {
      rule номер_правила {
         prefix подсеть_ipv6
      }
   }
}
```

Параметры

имя_списка

Множественный узел. Текстовый идентификатор для списка префиксов IPv6.

номер_правила

Множественный узел. Численный идентификатор правила.

подсеть_ipv6

Подсеть IPv6. Данному правилу будут соответствовать подсети, в точности совпадающие с данной подсетью. Допустимые значения указаны в таблице ниже:

Таблица 236 – Формат указания подсети IPv6

Значение	Описание
<x:x:x:x:x:x:x:x>/<0-128>	Сеть IPv6

В правиле списка префиксов указывается определенная подсеть с помощью атрибута prefix. Дополнительно возможно указание атрибутов ge и le (возможно использовать вместе в рамках одного правила).

Общая логика указания атрибутов описывается выражением prefix-value < ge-value <= le-value. Выделяются или ограничиваются определенные диапазоны подсетей, входящие в сеть с заданным префиксом.

- Атрибут ge определяет наибольшую подсеть в рамках указанного префикса (атрибутом prefix). В числовом значении (маски) это меньшее число. Таким образом определяется диапазон подсетей меньших или равных указанной.
- Атрибут le определяет наименьшую подсеть в рамках указанного префикса (атрибутом prefix). В числовом значении (маски) это большее число.Таким образом определяется диапазон подсетей больших или равных указанной.

Значение по умолчанию

Если подсеть не указана, считается, что все подсети соответствуют правилу.

Указания по использованию

Подсеть, указанная во входящих пакетах, сравнивается с данным значением; если подсеть в точности совпадает с подсетью, указанной в команде, то соответствие правилу считается найденным, и выполняется действие, указанное в данном правиле.

Форма **set** этой команды используется для указания подсети при определении политики фильтрации маршрутов.

Форма **delete** этой команды используется для удаления указанного префикса.

Форма **show** этой команды используется для отображения значения.

29.2.42 policy route-map <имя_карты>

Определение карты маршрутов при маршрутизации на основе политик.

Синтаксис

```
set policy route-map <имя_карты>
delete policy route-map <имя_карты>
show policy route-map <имя_карты>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route-map имя_карты {
   }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания карты маршрутов при маршрутизации на основе политик.

Форма **delete** этой команды используется для удаления карты маршрутов.

Форма **show** этой команды используется для отображения настройки карты маршрутов.

29.2.43 policy route-map <имя_карты> description <описание>

Ввод краткого описания карты маршрутов.

Синтаксис

```
set policy route-map <имя_карты> description <описание>
delete policy route-map <имя_карты> description
show policy route-map <имя_карты> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route-map имя_карты {
```

```
        description описание
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

описание

Краткое текстовое описание для карты маршрутов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания описания карты маршрутов.

Форма **delete** этой команды используется для удаления описания карты маршрутов.

Форма **show** этой команды используется для отображения описания карты маршрутов.

29.2.44 policy route-map <имя_карты> rule <номер_правила>

Создание правила карты маршрутов.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила>
delete policy route-map <имя_карты> rule <номер_правила>
show policy route-map <имя_карты> rule <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-map имя_карты {
        rule номер_правила {
        }
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила. Допустимые значения представлены в таблице ниже:

Таблица 237 – Допустимые номера правил

Значение	Описание
<1-65535>	Номер правила

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания правила карты маршрутов.

Форма **delete** этой команды используется для удаления правила карты маршрутов.

Форма **show** этой команды используется для отображения параметров настройки правила карты маршрутов.

29.2.45 policy route-map <имя_карты> rule <номер_правила> action <действие>

Указание действия, которое должно быть выполнено над пакетами, соответствующими правилу карты маршрутов.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> action <действие>
delete policy route-map <имя_карты> rule <номер_правила> action
show policy route-map <имя_карты> rule <номер_правила> action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route-map имя_карты {
      rule номер_правила {
         action действие
      }
   }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

действие

Обязательный. Указать, какое действие выполнять для пакетов, соответствующих данному правилу. Допустимые значения указаны в таблице ниже:

Таблица 238 – Возможные действия при соответствии правилу

Значение	Описание
deny	Пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений
permit	Пакеты, соответствующие данному правилу, передаются в дальнейшую обработку

Значение по умолчанию

Пакеты, соответствующие данному правилу,игнорируются без каких-либо действий и сообщений.

Указания по использованию

Форма **set** этой команды используется для определения действия, выполняемого над пакетом, удовлетворяющим критериям соответствия в данном правиле.

Форма **delete** этой команды используется для восстановления действия по умолчанию над пакетами, удовлетворяющими критериям соответствия.

Форма **show** этой команды используется для отображения параметров действия в данном правиле.

29.2.46 policy route-map <имя_карты> rule <номер_правила> call <имя_карты>

Вызов другой карты маршрутов.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> call <имя_карты>
delete policy route-map <имя_карты> rule <номер_правила> call
show policy route-map <имя_карты> rule <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route-map имя_карты {
      rule номер_правила {
         call имя_карты
      }
   }
}
```

Параметры

route-map *имя_карты*

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

call *имя_карты*

Текстовый идентификатор вызываемой карты маршрутов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Новая карта маршрутов вызывается после того, как все действия (set), указанные в текущем правиле карты маршрутов, выполнены. Если вызванная карта маршрутов возвращает permit, то политики проверки соответствия и выхода вызывающей карты маршрутов определяют дальнейшее поведение обычным образом. Если вызванная карта маршрутов возвращает deny, обработка карты маршрутов завершается, и пакет отклоняется независимо от любых дальнейших политик проверки соответствия или выхода.

Форма **set** этой команды используется для вызова другой карты маршрутов.

Форма **delete** этой команды используется для удаления оператора вызова из карты маршрутов.

Форма **show** этой команды используется для отображения параметров настройки правила карты маршрутов.

29.2.47 policy route-map <имя_карты> rule <номер_правила> continue <номер_правила>

Вызов другого правила в текущей карте маршрутов.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> continue <номер_правила>
delete policy route-map <имя_карты> rule <номер_правила> continue
show policy route-map <имя_карты> rule <номер_правила> continue
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-map имя_карты {
        rule номер_правила {
            continue имя_карты
        }
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

rule *номер_правила*

Множественный узел. Численный идентификатор правила.

continue *номер_правила*

Численный идентификатор вызываемого правила.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для вызова другого правила внутри текущей карты маршрутов. Новое правило карты маршрутов вызывается после того, как выполнены все действия (set), указанные в текущем правиле карты маршрутов.

Форма **delete** этой команды используется для удаления данного оператора из карты маршрутов.

Форма **show** этой команды используется для отображения параметров настройки правила карты маршрутов.

29.2.48 policy route-map <имя_карты> rule <номер_правила> description <описание>

Ввод краткого описания правила карты маршрутов.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> description <описание>
delete policy route-map <имя_карты> rule <номер_правила> description
show policy route-map <имя_карты> rule <номер_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-map имя_карты {
        rule номер_правила {
            description описание
        }
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

описание

Краткое текстовое описание правила карты маршрутов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания описания правила карты маршрутов.

Форма **delete** этой команды используется для удаления описания правила карты маршрутов.

Форма **show** этой команды используется для отображения описания правила карты маршрутов.

29.2.49 policy route-map <имя_карты> rule <номер_правила> match as-path <имя_списка>

Определение условия соответствия в карте маршрутов на основе списка путей AS.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> match as-path <имя_списка>
delete policy route-map <имя_карты> rule <номер_правила> match as-path
show policy route-map <имя_карты> rule <номер_правила> match as-path
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-map имя_карты {
        rule номер_правила {
            match {
                as-path имя_списка
            }
        }
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

имя_списка

Устанавливается соответствие списку путей AS. Список путей AS к этому моменту должен быть уже определен.

Значение по умолчанию

Если ни одно условие соответствия по путям AS не определено, фильтрация пакетов по пути AS не выполняется.

Указания по использованию

Если в правиле карты маршрутов определено более одного условия, для нахождения соответствия пакет должен соответствовать всем условиям. Если в правиле карты маршрутов не определено ни одного условия, считается, что правилу соответствуют все пакеты.

Форма **set** этой команды используется для определения условия соответствия, основанного на списке путей AS, в политике карты маршрутов.

Форма **delete** этой команды используется для удаления условия соответствия по пути AS.

Форма **show** этой команды используется для отображения настройки условия соответствия по пути AS.

29.2.50 policy route-map <имя_карты> rule <номер_правила> match community

Определение условия соответствия в карте маршрутов на основе сообществ BGP.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> match community [community-list <номер_списка> | exact-match]

delete policy route-map <имя_карты> rule <номер_правила> match community

show policy route-map <имя_карты> rule <номер_правила> match community
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-map имя_карты {
        rule номер_правила {
            match {
                community {
                    community-list номер_списка
                    exact-match
                }
            }
        }
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

community-list номер_списка

Численный идентификатор списка сообществ BGP. Политика сообществ BGP к этому моменту должна быть уже определена.

exact-match

Устанавливает режим строгого соответствия списку сообществ BGP. При использовании данного параметра обязательно должен быть определен community-list.

Значение по умолчанию

Если ни одно условие соответствия по спискам сообщества не определено, фильтрация пакетов по сообществам BGP не выполняется.

Указания по использованию

Если в правиле карты маршрутов определено более одного условия, для нахождения соответствия пакет должен соответствовать всем условиям. Если в правиле карты маршрутов не определено ни одного условия, считается, что правилу соответствуют все пакеты.

Форма **set** этой команды используется для определения условия соответствия, основанного на сообществах BGP, в политике карты маршрутов.

Форма **delete** этой команды используется для удаления условия соответствия по сообществу BGP.

Форма **show** этой команды используется для отображения настройки условия соответствия по сообществу BGP.

29.2.51 policy route-map <имя_карты> rule <номер_правила> match interface <интерфейс>

Определение условия соответствия в карте маршрутов на основе интерфейса первого транзитного узла.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> match interface <интерфейс>
delete policy route-map <имя_карты> rule <номер_правила> match interface
show policy route-map <имя_карты> rule <номер_правила> match interface
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-map имя_карты {
        rule номер_правила {
            match {
                interface интерфейс
            }
        }
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

интерфейс

Указание интерфейса для сопоставления. Поддерживается любой маршрутизируемый интерфейс. Интерфейс должен быть заранее определен в системе.

Значение по умолчанию

Если ни одно условие соответствия по интерфейсам не определено, фильтрация пакетов по интерфейсу не выполняется.

Указания по использованию

Если в правиле карты маршрутов определено более одного условия, для нахождения соответствия пакет должен соответствовать всем условиям. Если в правиле карты маршрутов не определено ни одного условия, считается, что правилу соответствуют все пакеты.

Форма **set** этой команды используется для определения условия соответствия, основанного на интерфейсе первого транзитного узла, в политике карты маршрутов.

Форма **delete** этой команды используется для удаления условия соответствия по интерфейсу.

Форма **show** этой команды используется для отображения настройки условия соответствия по интерфейсу.

29.2.52 policy route-map <имя_карты> rule <номер_правила> match ip address

Определение условия соответствия в карте маршрутов на основе IP-адреса.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> match ip address
[access-list <номер_списка> | prefix-list <имя_списка>]

delete policy route-map <имя_карты> rule <номер_правила> match ip address

show policy route-map <имя_карты> rule <номер_правила> match ip address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-map имя_карты {
        rule номер_правила {
            match {
                ip {
                    address {
                        access-list номер_списка
                        prefix-list имя_списка
                    }
                }
            }
        }
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

access-list номер_списка

IP-адрес отправителя или получателя маршрута проверяется на соответствие IP-адресам, разрешенным указанным списком доступа. Список доступа должен быть заранее определен.

prefix-list имя_списка

Подсеть отправителя или получателя маршрута проверяется на соответствие подсетям, разрешенным указанным списком префиксов. Список префиксов должен быть заранее определен.

Обязательно должен быть указан либо параметр access-list, либо параметр prefix-list.

Значение по умолчанию

Если ни одно условие соответствия по IP-адресам не определено, фильтрация пакетов по IP-адресам не выполняется.

Указания по использованию

Если в правиле карты маршрутов определено более одного условия, для нахождения соответствия пакет должен соответствовать всем условиям. Если в правиле карты маршрутов не определено ни одного условия, считается, что правилу соответствуют все пакеты.

Форма **set** этой команды используется для определения условия соответствия, основанного на IP-адресе, в политике карты маршрутов.

Форма **delete** этой команды используется для удаления условия соответствия по IP-адресу.

Форма **show** этой команды используется для отображения настройки условия соответствия по IP-адресу.

29.2.53 policy route-map <имя_карты> rule <номер_правила> match ip nexthop

Определение условия соответствия в карте маршрутов на основе адреса следующего транзитного узла.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> match ip nexthop [access-list <номер_списка> | prefix-list <имя_списка>]

delete policy route-map <имя_карты> rule <номер_правила> match ip nexthop

show policy route-map <имя_карты> rule <номер_правила> match ip nexthop
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-map имя_карты {
        rule номер_правила {
            match {
                ip {
                    nexthop {
                        access-list номер_списка
                        prefix-list имя_списка
                    }
                }
            }
        }
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

access-list номер_списка

IP-адрес следующего транзитного узла в маршруте проверяется на соответствие IP-адресам, разрешенным указанным списком доступа. Список доступа должен быть заранее определен.

prefix-list имя_списка

IP-адрес следующего транзитного узла в маршруте проверяется на соответствие IP-адресам, разрешенным указанным списком префиксов. Список префиксов должен быть заранее определен.

Обязательно должен быть указан либо параметр access-list, либо параметр prefix-list.

Значение по умолчанию

Если ни одно условие соответствия по следующему транзитному узлу не определено, фильтрация пакетов по следующему транзитному узлу не выполняется.

Указания по использованию

Если в правиле карты маршрутов определено более одного условия, для нахождения соответствия пакет должен соответствовать всем условиям. Если в правиле карты маршрутов не определено ни одного условия, считается, что правилу соответствуют все пакеты.

Форма **set** этой команды используется для определения условия соответствия, основанного на IP-адресе следующего транзитного узла, в политике карты маршрутов.

Форма **delete** этой команды используется для удаления условия соответствия по IP-адресу следующего транзитного узла.

Форма **show** этой команды используется для отображения настройки условия соответствия по IP-адресу следующего транзитного узла.

29.2.54 policy route-map <имя_карты> rule <номер_правила> match ip route-source

Определение условия соответствия в карте маршрутов на основе адреса, с которого объявляется маршрут.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> match ip route-source
[access-list <номер_списка> | prefix-list <имя_списка>]

delete policy route-map <имя_карты> rule <номер_правила> match ip route-
source

show policy route-map <имя_карты> rule <номер_правила> match ip route-source
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route-map имя_карты {
      rule номер_правила {
         match {
            ip {
               route-source {
                  access-list номер_списка
                  prefix-list имя_списка
               }
            }
         }
      }
```

```
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

access-list номер_списка

Считается найденным соответствие для маршрутов, объявляемых с адресов, содержащихся в указанном списке доступа. Список доступа должен быть заранее определен.

prefix-list имя_списка

Считается найденным соответствие для маршрутов, объявляемых с адресов, содержащихся в указанном списке префиксов. Список префиксов должен быть заранее определен.

Обязательно должен быть указан либо параметр access-list, либо параметр prefix-list.

Значение по умолчанию

Если ни одно условие соответствия по отправителю маршрутов не определено, фильтрация пакетов по отправителю маршрута не выполняется.

Указания по использованию

Если в правиле карты маршрутов определено более одного условия, для нахождения соответствия пакет должен соответствовать всем условиям. Если в правиле карты маршрутов не определено ни одного условия, считается, что правилу соответствуют все пакеты.

Форма **set** этой команды используется для определения условия соответствия, основанного на адресе, с которого объявляются маршруты (адресе отправителя маршрутов), в политике карты маршрутов.

Форма **delete** этой команды используется для удаления условия соответствия по адресу отправителя маршрута.

Форма **show** этой команды используется для отображения настройки условия соответствия по адресу отправителя маршрута.

29.2.55 policy route-map <имя_карты> rule <номер_правила> match ipv6 address

Определение условия соответствия в карте маршрутов на основе IPv6-адреса.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> match ipv6 address
[access-list6 <номер_списка> | prefix-list6 <имя_списка>]

delete policy route-map <имя_карты> rule <номер_правила> match ipv6 address

show policy route-map <имя_карты> rule <номер_правила> match ipv6 address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-map имя_карты {
        rule номер_правила {
            match {
                ipv6 {
                    address {
                        access-list6 номер_списка
```

```
                    prefix-list6 имя_списка
                }
            }
        }
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

access-list6 номер_списка

IPv6-адрес отправителя или получателя маршрута проверяется на соответствие IPv6-адресам, разрешенным указанным списком доступа. Список доступа должен быть заранее определен.

prefix-list6 имя_списка

Подсеть отправителя или получателя маршрута проверяется на соответствие подсетям, разрешенным указанным списком префиксов. Список префиксов должен быть заранее определен.

Обязательно должен быть указан либо параметр access-list6, либо параметр prefix-list6.

Значение по умолчанию

Если ни одно условие соответствия по IPv6-адресу не определено, фильтрация пакетов по IPv6-адресам не выполняется.

Указания по использованию

Если в правиле карты маршрутов определено более одного условия, для нахождения соответствия пакет должен соответствовать всем условиям. Если в правиле карты маршрутов не определено ни одного условия, считается, что правилу соответствуют все пакеты.

Форма **set** этой команды используется для определения условия соответствия, основанного на IPv6-адресе, в политике карты маршрутов.

Форма **delete** этой команды используется для удаления условия соответствия по IPv6-адресу.

Форма **show** этой команды используется для отображения настройки условия соответствия по IPv6-адресу.

29.2.56 policy route-map <имя_карты> rule <номер_правила> match ipv6 nexthop

Определение условия соответствия в карте маршрутов на основе IPv6-адреса следующего транзитного узла.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> match ipv6 nexthop
[access-list6 <номер_списка> | prefix-list6 <имя_списка>]

delete policy route-map <имя_карты> rule <номер_правила> match ipv6 nexthop

show policy route-map <имя_карты> rule <номер_правила> match ipv6 nexthop
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-map имя_карты {
        rule номер_правила {
```

```
            match {
                ipv6 {
                    nexthop {
                        access-list6 номер_списка
                        prefix-list6 имя_списка
                    }
                }
            }
        }
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

access-list6 номер_списка

IPv6-адрес следующего транзитного узла в маршруте проверяется на соответствие IPv6-адресам, разрешенным указанным списком доступа. Список доступа должен быть заранее определен.

prefix-list6 имя_списка

IPv6-адрес следующего транзитного узла в маршруте проверяется на соответствие IPv6-адресам, разрешенным указанным списком префиксов. Список префиксов должен быть заранее определен.

Обязательно должен быть указан либо параметр access-list6, либо параметр prefix-list6.

Значение по умолчанию

Если ни одно условие соответствия по следующему транзитному узлу не определено, фильтрация пакетов по следующему транзитному узлу не выполняется.

Указания по использованию

Если в правиле карты маршрутов определено более одного условия, для нахождения соответствия пакет должен соответствовать всем условиям. Если в правиле карты маршрутов не определено ни одного условия, считается, что правилу соответствуют все пакеты.

Форма **set** этой команды используется для определения условия соответствия, основанного на IPv6-адресе следующего транзитного узла, в политике карты маршрутов.

Форма **delete** этой команды используется для удаления условия соответствия по IPv6-адресу следующего транзитного узла.

Форма **show** этой команды используется для отображения настройки условия соответствия по IPv6-адресу следующего транзитного узла.

29.2.57 policy route-map <имя_карты> rule <номер_правила> match metric <метрика>

Определение условия соответствия в карте маршрутов на основе метрики маршрута.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> match metric <метрика>
delete policy route-map <имя_карты> rule <номер_правила> match metric
show policy route-map <имя_карты> rule <номер_правила> match metric
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-map имя_карты {
        rule номер_правила {
            match {
                metric метрика
            }
        }
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

метрика

Число, представляющее метрику маршрута. Допустимые значения представлены в таблице ниже:

Таблица 239 – Возможные значения метрики маршрута

Значение	Описание
<1-65535>	Метрика маршрута

Значение по умолчанию

Если ни одно условие соответствия по метрике не определено, фильтрация пакетов по метрике не выполняется.

Указания по использованию

Если в правиле карты маршрутов определено более одного условия, для нахождения соответствия пакет должен соответствовать всем условиям. Если в правиле карты маршрутов не определено ни одного условия, считается, что правилу соответствуют все пакеты.

Форма **set** этой команды используется для определения условия соответствия, основанного на метрике маршрута, в политике карты маршрутов.

Форма **delete** этой команды используется для удаления условия соответствия по адресу отправителя маршрута.

Форма **show** этой команды используется для отображения настройки условия соответствия по адресу отправителя маршрута.

29.2.58 policy route-map <имя_карты> rule <номер_правила> match origin <способ_получения>

Определение условия соответствия в карте маршрутов на основе способа получения маршрута.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> match origin <способ_получения>

delete policy route-map <имя_карты> rule <номер_правила> match origin

show policy route-map <имя_карты> rule <номер_правила> match origin
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-map имя_карты {
        rule номер_правила {
            match {
                origin способ_получения
            }
        }
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

способ_получения

Указывает способ получения маршрута. Допустимые значения представлены в таблице ниже:

Таблица 240

Значение	Описание
egp	Считается найденным соответствие для маршрутов, полученных по протоколу EGP.
igp	Считается найденным соответствие для маршрутов, полученных по протоколу IGP.
incomplete	Считается найденным соответствие для маршрутов, код BGP способа получения которых неполон.

Значение по умолчанию

Если ни одно условие соответствия по способу получения не определено, фильтрация пакетов по способу получения не выполняется.

Указания по использованию

Если в правиле карты маршрутов определено более одного условия, для нахождения соответствия пакет должен соответствовать всем условиям. Если в правиле карты маршрутов не определено ни одного условия, считается, что правилу соответствуют все пакеты.

Форма **set** этой команды используется для определения условия соответствия, основанного на коде BGP способа получения, в политике карты маршрутов.

Форма **delete** этой команды используется для удаления условия соответствия по коду способа получения.

Форма **show** этой команды используется для отображения настройки условия соответствия по коду способа получения.

29.2.59 policy route-map <имя_карты> rule <номер_правила> match peer

Определение условия соответствия в карте маршрутов на основе IP-адреса равноправного узла.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> match peer [ipv4-адрес
| local]

delete policy route-map <имя_карты> rule <номер_правила> match peer

show policy route-map <имя_карты> rule <номер_правила> match peer
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route-map имя_карты {
      rule номер_правила {
         match {
            peer ipv4-адрес | local
         }
      }
   }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

ipv4-адрес

IPv4-адрес. На соответствие этому адресу проверяется адрес равноправного узла в маршруте.

local

При указании данного параметра сопоставление будет производиться не с равноправным узлом, а с собственными статическими и перераспределенными маршрутами системы.

Значение по умолчанию

Если ни одно условие соответствия не определено, фильтрация пакетов не выполняется.

Указания по использованию

Если в правиле карты маршрутов определено более одного условия, для нахождения соответствия пакет должен соответствовать всем условиям. Если в правиле карты маршрутов не определено ни одного условия, считается, что правилу соответствуют все пакеты.

Форма **set** этой команды используется для определения условия соответствия, основанного на IP-адресе равноправного узла, в политике карты маршрутов.

Форма **delete** этой команды используется для удаления условия соответствия по адресу равноправного узла.

Форма **show** этой команды используется для отображения настройки условия соответствия по адресу равноправного узла.

29.2.60 policy route-map <имя_карты> rule <номер_правила> match tag <тег>

Определение условия соответствия в карте маршрутов на основе тега OSPF.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> match tag <тег>
delete policy route-map <имя_карты> rule <номер_правила> match tag
show policy route-map <имя_карты> rule <номер_правила> match tag
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route-map имя_карты {
```

```
        rule номер_правила {
           match {
              tag тег
           }
        }
     }
  }
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

тег

Число, представляющее тег OSPF. На соответствие этому значению проверяется содержимое поля внешнего тега LSA (Link-State Advertisement, объявление состояния канала) протокола OSPF в маршруте. Допустимые значения представлены в таблице ниже:

Таблица 241 – Возможные значения тегов маршрута

Значение	Описание
<1-65535>	Тег маршрута

Значение по умолчанию

Если ни одно условие соответствия по тегу не определено, фильтрация пакетов по тегу не выполняется.

Указания по использованию

Если в правиле карты маршрутов определено более одного условия, для нахождения соответствия пакет должен соответствовать всем условиям. Если в правиле карты маршрутов не определено ни одного условия, считается, что правилу соответствуют все пакеты.

Форма **set** этой команды используется для определения условия соответствия, основанного на теге OSPF, в политике карты маршрутов.

Форма **delete** этой команды используется для удаления условия соответствия по тегу OSPF.

Форма **show** этой команды используется для отображения настройки условия соответствия по тегу OSPF.

29.2.61 policy route-map <имя_карты> rule <номер_правила> on-match

Указание альтернативной политики выхода в карте маршрутов.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> on-match <действие>
delete policy route-map <имя_карты> rule <номер_правила> on-match
show policy route-map <имя_карты> rule <номер_правила> on-match
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route-map имя_карты {
      rule номер_правила {
         on-match {
            goto номер_правила
```

```
                next
            }
        }
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

goto <номер_правила>

Выход из текущего правила карты маршрутов, вызов правила, указанного данным параметром, и его выполнение. Переход на предшествующее правило списка маршрутов не разрешается.

next

Выход из текущего правила карты маршрутов, вызов следующего правила в последовательности и его выполнение.

Значение по умолчанию

Отсутствует.

Указания по использованию

Обычно при нахождении соответствия карте маршрутов происходит выход из карты маршрутов и разрешение маршрута. Данная команда позволяет указать альтернативную политику выхода путем передачи управления на указанное правило карты маршрутов или на следующее правило в последовательности.

Форма **set** этой команды используется для определения политики выхода в элементе карты маршрутов путем указания правила карты маршрутов, которое должно быть выполнено в случае соответствия.

Форма **delete** этой команды используется для удаления политики выхода.

Форма **show** этой команды используется для отображения настройки политики выхода из карты маршрутов.

29.2.62 olicy route-map <имя_карты> rule <номер_правила> set aggregator

Изменение атрибута агрегатора протокола BGP для маршрута.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> set aggregator [as <номер_as> | ip <ipv4-адрес>]
delete policy route-map <имя_карты> rule <номер_правила> set aggregator
show policy route-map <имя_карты> rule <номер_правила> set
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-map имя_карты {
        rule номер_правила {
            set {
                as номер_as
                ip ipv4-адрес
            }
```

```
        }
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

as номер_as

Изменение номера автономной системы агрегатора BGP в маршруте на указанное значение. Диапазон допустимых значений представлен в таблице ниже:

Таблица 242 – Допустимые номера AS протокола BGP

Значение	Описание
<1-65535>	Номер AS

ip ipv4-адрес

Изменение IP-адреса агрегатора BGP в маршруте на указанный IPv4-адрес.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для изменения атрибута агрегатора маршрута. Когда все условия соответствий, указанные в правиле карты маршрутов, удовлетворены, происходит изменение атрибута агрегатора указанным образом.

Форма **delete** этой команды используется для удаления данного оператора из правила карты маршрутов.

Форма **show** этой команды используется для отображения настройки оператора set для карт маршрутов.

29.2.63 policy route-map <имя_карты> rule <номер_правила> set as-path-prepend <добавляемая_строка>

Установка строки или ее добавление в начало пути AS для маршрута.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> set as-path-prepend <добавляемая_строка>
delete policy route-map <имя_карты> rule <номер_правила> set as-path-prepend
show policy route-map <имя_карты> rule <номер_правила> set
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-map имя_карты {
        rule номер_правила {
            set {
                as-path-pretend добавляемая_строка
            }
        }
    }
```

```
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

добавляемая_строка

Строка, представляющая путь AS.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для добавления строки в начало списка путей AS в маршруте. Когда все условия соответствий, указанные в правиле карты маршрутов, удовлетворены, указанная строка добавляется в начало пути AS в маршруте.

Форма **delete** этой команды используется для удаления данного оператора из правила карты маршрутов.

Форма **show** этой команды используется для отображения настройки оператора set для карт маршрутов.

29.2.64 policy route-map <имя_карты> rule <номер_правила> set atomic-aggregate

Установка атрибута atomic-aggregate протокола BGP в маршруте.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> set atomic-aggregate
delete policy route-map <имя_карты> rule <номер_правила> set atomic-aggregate
show policy route-map <имя_карты> rule <номер_правила> set
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route-map имя_карты {
      rule номер_правила {
         set {
            atomic-aggregate
         }
      }
   }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для установки атрибута атомарного агрегата BGP в маршруте. Когда все условия соответствий, указанные в правиле карты маршрутов, удовлетворены, происходит изменение атрибута атомарного агрегата указанным образом.

Форма **delete** этой команды используется для удаления данного оператора из правила карты маршрутов.

Форма **show** этой команды используется для отображения настройки оператора set для карт маршрутов.

29.2.65 policy route-map <имя_карты> rule <номер_правила> set comm-list

Изменение списка сообщества BGP в маршруте.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> set comm-list [comm-list <номер_списка> | delete]

delete policy route-map <имя_карты> rule <номер_правила> set comm-list

show policy route-map <имя_карты> rule <номер_правила> set
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-map имя_карты {
        rule номер_правила {
            set {
                comm-list {
                    comm-list номер_списка
                    delete
                }
            }
        }
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

comm-list номер_списка

Добавление сообществ, перечисленных в указанном списке сообществ, в список сообществ маршрута. Список сообществ к моменту выдачи команды должен быть заранее определен.

delete

Удаление сообществ, перечисленных в указанном списке сообществ, в список сообществ маршрута. Используется совместно с параметром *comm-list номер_списка*.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для изменения списка сообществ BGP в маршруте. Когда все условия соответствий, указанные в правиле карты маршрутов, удовлетворены, происходит изменение списка сообществ указанным образом.

Форма **delete** этой команды используется для удаления данного оператора из правила карты маршрутов.

Форма **show** этой команды используется для отображения настройки оператора **set** для карт маршрутов.

29.2.66 policy route-map <имя_карты> rule <номер_правила> set community

Изменение атрибута communities BGP в маршруте.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> set community ["[additive] <сообщество>" | none]

delete policy route-map <имя_карты> rule <номер_правила> set community

show policy route-map <имя_карты> rule <номер_правила> set
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-map имя_карты {
        rule номер_правила {
            set {
                community "[additive] сообщество" | none
            }
        }
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

additive

Добавление указанного сообщества к существующим сообществам в пути. Если указано ключевое слово additive, необходимо использовать двойные кавычки.

сообщество

Сообщество BGP. Допустимые значения представлены в таблице ниже:

Таблица 243 – Поддерживаемые форматы указания сообществ BGP.

Значение	Описание
<aa:nn>	Номер сообщества
local-AS	Зарезервированное значение согласно RFC 1997. При указании маршруты анонсируются только в локальной AS (NO_EXPORT_SUBCONFED).
no-export	Зарезервированное значение согласно RFC 1997. При указании маршруты не анонсируются за пределы данной AS (NO_EXPORT).
no-advertise	Зарезервированное значение согласно RFC 1997. При указании маршруты не анонсируются другим BGP-соседям (NO_ADVERTISE).

internet	Специализированное значение сообщества 0:0, что равносильно соответствию любым сообществам.

none

Удаление атрибута сообществ из информации анонсов BGP.

Значение по умолчанию

Если ключевое слово additive не используется, выполняется замена существующих сообществ в маршруте указанным сообществом.

Указания по использованию

Форма **set** этой команды используется для изменения атрибута сообществ BGP в маршруте. Когда все условия соответствий, указанные в правиле карты маршрутов, удовлетворены, происходит изменение атрибута сообществ указанным образом.

Форма **delete** этой команды используется для удаления данного оператора из правила карты маршрутов.

Форма **show** этой команды используется для отображения настройки оператора set для карт маршрутов.

29.2.67 policy route-map <имя_карты> rule <номер_правила> set ip-next-hop <ipv4-адрес>

Изменение получателя следующего транзитного узла маршрута.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> set ip-next-hop <ipv4-адрес>
delete policy route-map <имя_карты> rule <номер_правила> set ip-next-hop
show policy route-map <имя_карты> rule <номер_правила> set
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route-map имя_карты {
      rule номер_правила {
         set {
            ip-next-hop ipv4-адрес
         }
      }
   }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

ipv4-адрес

Устанавливает адрес следующего транзитного узла.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для изменения получателя следующего транзитного узла для пакетов, проходящих через карту маршрутов. Когда все условия соответствий, указанные в правиле карты маршрутов, удовлетворены, происходит изменение следующего транзитного узла маршрута указанным образом.

Форма **delete** этой команды используется для удаления данного оператора из правила карты маршрутов.

Форма **show** этой команды используется для отображения настройки оператора set для карт маршрутов.

29.2.68 policy route-map <имя_карты> rule <номер_правила> set local-preference <local-pref>

Изменение атрибута local-pref BGP в маршруте.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> set local-preference
<local-pref>

delete policy route-map <имя_карты> rule <номер_правила> set local-preference

show policy route-map <имя_карты> rule <номер_правила> set
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-map имя_карты {
        rule номер_правила {
            set {
                local-preference local-pref
            }
        }
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

local-pref

Новое значение для атрибута локального предпочтения маршрута BGP. Допустимые значения представлены в таблице ниже:

Таблица 244 – Значения атрибута local-pref.

Значение	Описание
<0-4294967295>	Значение атрибута local-pref (локальная предпочтительность)

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для изменения атрибута local-pref BGP у пакетов, проходящих через карту маршрутов. Когда все условия соответствий, указанные в правиле карты маршрутов, удовлетворены, происходит изменение атрибута local-pref маршрута указанным образом.

Форма **delete** этой команды используется для удаления данного оператора из правила карты маршрутов.

Форма **show** этой команды используется для отображения настройки оператора set для карт маршрутов.

29.2.69 policy route-map <имя_карты> rule <номер_правила> set metric <метрика>

Изменение метрики маршрута.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> set metric <метрика>
delete policy route-map <имя_карты> rule <номер_правила> set metric
show policy route-map <имя_карты> rule <номер_правила> set
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route-map имя_карты {
      rule номер_правила {
         set {
            metric метрика
         }
      }
   }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

метрика

Число, представляющее новую метрику, которая должна быть использована в маршруте. Допустимые значение представлены в таблице ниже:

Таблица 245 – Возможные значения для указания метрики маршрутов.

Значение	Описание
<+metric>	Увеличение значения мерики маршрута на указанную величину
<0-4294967295>	Указание значения метрики маршрута.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для изменения метрики маршрута у пакетов, проходящих через карту маршрутов. Когда все условия соответствий, указанные в правиле карты маршрутов, удовлетворены, происходит изменение метрики маршрута указанным образом.

Форма **delete** этой команды используется для удаления данного оператора из правила карты маршрутов.

Форма **show** этой команды используется для отображения настройки оператора set для карт маршрутов.

29.2.70 policy route-map <имя_карты> rule <номер_правила> set metric-type <тип>

Указание типа внешней метрики OSPF для маршрута.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> set metric-type <тип>
delete policy route-map <имя_карты> rule <номер_правила> set metric-type
show policy route-map <имя_карты> rule <номер_правила> set
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route-map имя_карты {
      rule номер_правила {
         set {
            metric-type тип
         }
      }
   }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

тип

Указание типа используемое внешней метрики протокола OSPF. Допустимые значения представлены в таблице ниже:

Таблица 246 – Типы метрики OSPF.

Значение	Описание
type-1	В этой метрике при вычислении стоимости доступа ко внешней сети используются как внешние, так и внутренние стоимости.
type-2	В этой метрике при вычислении стоимости доступа ко внешней сети используются только внешние стоимости.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания типа метрики, которая должна использоваться протоколом OSPF для вычисления стоимости доступа ко внешней сети.

Форма set этой команды используется для указания типа внешней метрики OSPF для маршрута.

Форма **delete** этой команды используется для удаления типа метрики.

Форма **show** этой команды используется для отображения типа метрики.

29.2.71 policy route-map <имя_карты> rule <номер_правила> set origin <способ_получения>

Изменение кода BGP способа получения маршрута.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> set origin <способ получения>
delete policy route-map <имя_карты> rule <номер_правила> set origin
show policy route-map <имя_карты> rule <номер_правила> set
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-map имя_карты {
        rule номер_правила {
            set {
                origin способ_получения
            }
        }
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

способ_получения

Указывает способ получения маршрута. Допустимые значения представлены в таблице ниже:

Таблица 247

Значение	Описание
egp	Считается найденным соответствие для маршрутов, полученных по протоколу EGP.
igp	Считается найденным соответствие для маршрутов, полученных по протоколу IGP.
incomplete	Считается найденным соответствие для маршрутов, код BGP способа получения которых неполон.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для установки кода способа получения BGP у пакетов, проходящих через карту маршрутов. Когда все условия соответствий, указанные в правиле карты маршрутов, удовлетворены, происходит изменение кода получения BGP указанным образом.

Форма **delete** этой команды используется для удаления данного оператора из правила карты маршрутов.

Форма **show** этой команды используется для отображения настройки оператора set для карт маршрутов.

29.2.72 policy route-map <имя_карты> rule <номер_правила> set originator-id <ipv4-адрес>

Изменение атрибута идентификатора отправителя BGP для маршрута.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> set originator-id <ipv4-адрес>
```

```
delete policy route-map <имя_карты> rule <номер_правила> set originator-id
show policy route-map <имя_карты> rule <номер_правила> set
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route-map имя_карты {
      rule номер_правила {
         set {
            originator-id ipv4-адрес
         }
      }
   }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

ipv4-адрес

IPv4-адрес, который следует использовать в качестве нового идентификатора отправителя.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для установки идентификатора отправителя BGP у пакетов, проходящих через карту маршрутов. Когда все условия соответствий, указанные в правиле карты маршрутов, удовлетворены, происходит изменение идентификатора отправителя BGP указанным образом.

Форма **delete** этой команды используется для удаления данного оператора из правила карты маршрутов.

Форма **show** этой команды используется для отображения настройки оператора set для карт маршрутов.

29.2.73 policy route-map <имя_карты> rule <номер_правила> set tag <тег>

Изменение значения тега OSPF маршрута.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> set tag <тег>
delete policy route-map <имя_карты> rule <номер_правила> set tag
show policy route-map <имя_карты> rule <номер_правила> set tag
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route-map имя_карты {
      rule номер_правила {
         set {
```

```
            tag тег
        }
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

тег

Число, представляющее новое значение поля внешнего тега LSA протокола OSPF. Допустимые значения представлены в таблице ниже:

Таблица 248 – Возможные значения тега OSPF маршрута.

Значение	Описание
<1-65535>	Значение тега OSPF маршрута.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для установки значения тега OSPF у пакетов, проходящих через карту маршрутов. Когда все условия соответствий, указанные в правиле карты маршрутов, удовлетворены, происходит изменение тега маршрута указанным образом.

Форма **delete** этой команды используется для удаления данного оператора из правила карты маршрутов.

Форма **show** этой команды используется для отображения настройки оператора set для карт маршрутов.

29.2.74 policy route-map <имя_карты> rule <номер_правила> set weight <вес>

Изменение веса BGP маршрута.

Синтаксис

```
set policy route-map <имя_карты> rule <номер_правила> set weight <вес>
delete policy route-map <имя_карты> rule <номер_правила> set weight
show policy route-map <имя_карты> rule <номер_правила> set
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-map имя_карты {
        rule номер_правила {
            set {
                weight вес
            }
        }
    }
}
```

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

номер_правила

Множественный узел. Численный идентификатор правила.

вес

Вес BGP для записи в таблицу маршрутизации. Допустимые значения представлены в таблице ниже:

Таблица 249 – Возможные значения веса маршрута BGP.

Значение	Описание
<0-4294967295>	Вес маршрута BGP.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для установки веса BGP у маршрутов. Когда все условия соответствий, указанные в правиле карты маршрутов, удовлетворены, происходит изменение веса маршрута указанным образом.

Форма **delete** этой команды используется для удаления данного оператора из правила карты маршрутов.

Форма **show** этой команды используется для отображения настройки оператора set карт маршрутов.

29.2.75 policy show access-list

Отображение информации о списках доступа IPv4.

Синтаксис

```
policy show access-list [<номер_списка> | all]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

номер_списка

Отобразить информацию только об указанном списке доступа.

all

Отобразить информацию обо всех сконфигурированных списках доступа IPv4.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения списков доступа IPv4.

Примеры

В примере приведен образец вывода сконфигурированного списка доступа IPv4 100.

Пример 296 – Вывод списка доступа IPv4

```
admin@edge:~$ policy show access-list 100
ZEBRA:
Extended IP access list 100
    deny   ip any any
RIP:
Extended IP access list 100
    deny   ip any any
RIPNG:
Extended IP access list 100
    deny   ip any any
OSPF:
Extended IP access list 100
    deny   ip any any
OSPF6:
Extended IP access list 100
    deny   ip any any
BGP:
Extended IP access list 100
    deny   ip any any
```

29.2.76 policy show access-list6

Отображение информации о списках доступа IPv6.

Синтаксис

```
policy show access-list [<номер_списка> | all]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

номер_списка

Отобразить информацию только об указанном списке доступа.

all

Отобразить информацию обо всех сконфигурированных списках доступа IPv6.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения списков доступа IPv6.

Примеры

В примере приведен образец вывода сконфигурированного списка доступа IPv6 ACC_LIST_1.

Пример 297 – Вывод списка доступа IPv6

```
admin@edge:~$ policy show access-list6 ACC_LIST_1
ZEBRA:
Zebra IPv6 access list ACC_LIST_1
    permit any
RIP:
Zebra IPv6 access list ACC_LIST_1
    permit any
RIPNG:
Zebra IPv6 access list ACC_LIST_1
    permit any
OSPF:
Zebra IPv6 access list ACC_LIST_1
    permit any
OSPF6:
Zebra IPv6 access list ACC_LIST_1
    permit any
BGP:
Zebra IPv6 access list ACC_LIST_1
    permit any
```

29.2.77 policy show as-path-list

Отображение информации о путевых списках AS.

Синтаксис

```
policy show as-path-access-list [<имя_списка> | all]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_списка

Отобразить информацию только об указанном путевом списке AS.

all

Отобразить информацию обо всех сконфигурированных путевых списках AS.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения информации о путевых списках AS.

Примеры

В примере приведен образец вывода путевого списка AS TEST.

Пример 298 – Вывод информации о путевом списке AS

```
admin@edge:~$ policy show as-path-list TEST
AS path access list TEST
    deny 64500
    permit 64496
```

29.2.78 policy show community-list

Отображение информации о списках сообществ.

Синтаксис

```
policy show community-list [<имя_списка> | all]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_списка

Отобразить информацию только об указанном списке сообществ.

all

Отобразить информацию обо всех сконфигурированных списках сообществ.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения информации о списках сообществ.

Примеры

В примере приведен образец вывода списков сообществ.

Пример 299 – Вывод информации о списках сообществ

```
admin@edge:~$ policy show community-list all
Community (expanded) access list 150
    deny internet
    permit local-AS
```

29.2.79 policy show prefix-list

Отображение информации о списках префиксов IPv4.

Синтаксис

```
policy show prefix-list [<имя_списка> [detail | network <ipv4-сеть> | rule <номер_правила> | summary] | all [detail | summary]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_списка

Отобразить информацию только об указанном списке префиксов IPv4.

network ipv4-сеть

Отобразить информацию об указанной сети списка префиксов IPv4.

rule номер_правила

Отобразить информацию об указанном правиле списка префиксов IPv4.

all

Отобразить информацию обо всех сконфигурированных списках префиксов IPv4.

detail

Отобразить подробную информацию об указанном списке префиксов или обо всех сконфигурированных списках префиксов IPv4.

summary

Отобразить сводку по указанному списку префиксов или по всем сконфигурированным спискам префиксов IPv4.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения информации о списках префиксов IPv4.

Примеры

В примере приведен образец вывода информации о настроенных списках префиксов.

Пример 300 – Вывод информации о списках префиксов IPv4

```
admin@edge:~$ policy show prefix-list all
ZEBRA: ip prefix-list ALLOW-PREFIXES: 1 entries
   seq 10 permit 192.168.200.0/24
ZEBRA: ip prefix-list DENY-RANGE-PREFIXES: 1 entries
   seq 10 permit 192.168.213.0/23 le 32
RIP: ip prefix-list ALLOW-PREFIXES: 1 entries
   seq 10 permit 192.168.200.0/24
RIP: ip prefix-list DENY-RANGE-PREFIXES: 1 entries
   seq 10 permit 192.168.213.0/23 le 32
OSPF: ip prefix-list ALLOW-PREFIXES: 1 entries
   seq 10 permit 192.168.200.0/24
OSPF: ip prefix-list DENY-RANGE-PREFIXES: 1 entries
   seq 10 permit 192.168.213.0/23 le 32
BGP: ip prefix-list ALLOW-PREFIXES: 1 entries
   seq 10 permit 192.168.200.0/24
BGP: ip prefix-list DENY-RANGE-PREFIXES: 1 entries
   seq 10 permit 192.168.213.0/23 le 32
```

29.2.80 policy show prefix-list6

Отображение информации о списках префиксов IPv6.

Синтаксис

```
policy show prefix-list6 [<имя_списка> [detail | network <ipv6-сеть> | rule <номер_правила> | summary] | all [detail | summary]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_списка

Отобразить информацию только об указанном списке префиксов IPv6.

network ipv6-сеть

Отобразить информацию об указанной сети списка префиксов IPv6.

rule номер_правила

Отобразить информацию об указанном правиле списка префиксов IPv6.

all

Отобразить информацию обо всех сконфигурированных списках префиксов IPv6.

detail

Отобразить подробную информацию об указанном списке префиксов или обо всех сконфигурированных списках префиксов IPv6.

summary

Отобразить сводку по указанному списку префиксов или по всем сконфигурированным спискам префиксов IPv6.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения информации о списках префиксов IPv6.

29.2.81 show ip protocol

Отображение карт маршрутов IP по протоколам.

Синтаксис

```
show ip protocol
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения карт маршрутов по протоколам.

29.2.82 policy show route-map

Отображение сведений карты маршрутов.

Синтаксис

```
policy show route-map [<имя_карты> | all]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_карты

Множественный узел. Текстовый идентификатор карты маршрутов.

all

Отображение сведений обо всех сконфигурированных картах маршрутов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения сведений карты маршрутов.

Примеры

В примере приведен образец вывода сведений карты маршрутов.

Пример 301 – Вывод сведений карты маршрутов.

```
admin@edge01:~$ policy show route-map test
ZEBRA:
route-map test, permit, sequence 10
  Match clauses:
    ip address 100
  Set clauses:
  Call clause:
  Action:
    Exit routemap
RIP:
route-map test, permit, sequence 10
  Match clauses:
    ip address 100
  Set clauses:
    ip next-hop 192.168.10.1
  Call clause:
  Action:
    Exit routemap
RIPNG:
route-map test, permit, sequence 10
  Match clauses:
  Set clauses:
    metric 150
  Call clause:
  Action:
    Exit routemap
OSPF:
route-map test, permit, sequence 10
  Match clauses:
    ip address 100
  Set clauses:
    metric 150
  Call clause:
  Action:
    Exit routemap
OSPF6:
route-map test, permit, sequence 10
  Match clauses:
  Set clauses:
    metric 150
  Call clause:
  Action:
    Exit routemap
BGP:
route-map test, permit, sequence 10
  Match clauses:
    ip address 100
  Set clauses:
    metric 150
    weight 4294967295
    ip next-hop 192.168.10.1
  Call clause:
  Action:
    Exit routemap
```

30 Политики фильтрации ARP

30.1 Команды настройки

Режим настройки	
interfaces <интерфейс> policy <направление> arp <имя_политики>	Применение политики фильтрации ARP к указанному интерфейсу.
policy arp <имя_политики>	Определение имени политики фильтрации ARP.
policy arp <имя_политики> default-action <действие>	Определение для указанной политики фильтрации ARP действия по умолчанию.
policy arp <имя_политики> description <описание>	Создание текстового описания для указанной политики фильтрации ARP.
policy arp <имя_политики> rule <номер_правила>	Определение правила политики фильтрации ARP.
policy arp <имя_политики> rule <номер_правила> action <действие>	Указание действия для правила политики фильтрации ARP.
policy arp <имя_политики> rule <номер_правила> destination ip <ipv4-адрес>	Указание IP-адреса или подсети назначения для правила политики фильтрации ARP.
policy arp <имя_политики> rule <номер_правила> destination mac <mac-адрес>	Указание MAC-адреса назначения для правила политики фильтрации ARP.
policy arp <имя_политики> rule <номер_правила> hardware-length <длина>	Указание длины физического адреса в байтах для правила политики фильтрации ARP.
policy arp <имя_политики> rule <номер_правила> hardware-type <протокол>	Указание протокола канального уровня для правила политики фильтрации ARP.
policy arp <имя_политики> rule <номер_правила> operation <код_операции>	Указание кода операции для правила политики фильтрации ARP.
policy arp <имя_политики> rule <номер_правила> source ip <ipv4-адрес>	Указание IP-адреса или подсети источника (отправителя) для правила политики фильтрации ARP.
policy arp <имя_политики> rule <номер_правила> source mac <mac-адрес>	Указание MAC-адреса источника (отправителя) для правила политики фильтрации ARP.
policy arp <имя_политики> rule <номер_правила> protocol-type <протокол>	Указание протокола сетевого уровня для правила политики фильтрации ARP.
Эксплуатационные команды	
policy clear arp <имя_политики>	Очистка статистики политики фильтрации ARP.
policy show arp <имя_политики>	Вывод сведений и статистики политики фильтрации ARP.
policy show arp <имя_политики> rule <номер_правила>	Вывод сведений и статистики по указанному правилу политики фильтрации ARP.

30.1.1 interfaces <интерфейс> policy <направление> arp <имя_политики>

Применение политики фильтрации ARP к указанному интерфейсу.

Синтаксис

```
set interfaces <интерфейс> policy <направление> arp <имя_политики>
delete interfaces <интерфейс> policy <направление> arp
show interfaces <интерфейс> policy <направление> arp
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
   policy {
      направление {
         arp имя_политики
```

```
            }
        }
    }
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже в разделе Указания по использованию.

направление

Обязательный. Направление трафика, к которому применяется политика фильтрации ARP. Допустимые значения указаны в таблице ниже:

Таблица 250– Направления трафика

Значение	Описание
in	Транзитный трафик, принимаемый на указанном интерфейсе
out	Транзитный трафик, отправляемый с указанного интерфейса
local	Трафик, принятый на интерфейсе, предназначенный для локальной системы.

имя_политики

Имя политики фильтрации ARP, применяемой к данному интерфейсу.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для применения политики фильтрации ARP к интерфейсу.

Фильтрация транзитного трафика или трафика, предназначенного для локальной системы, не осуществляется до тех пор, пока политика межсетевого экранирования не будет применена к интерфейсу (реальному или виртуальному) с использованием данной команды.

На каждом интерфейсе можно применить до трех политик межсетевого экранирования: одну как фильтр транзитного трафика, принимаемого на интерфейсе (in), одну – как фильтр транзитного трафика, покидающего интерфейс (out) и одну – как фильтр трафика, предназначенного для локальной системы (local).

В приведенной ниже таблице показаны типы поддерживаемых интерфейсов и синтаксис.

Таблица 251– Типы интерфейсов

Тип интерфейса	Синтаксис
Агрегирование каналов	bonding bondx
Виртуальный интерфейс агрегированных каналов	bonding bondx vif идентификатор_vlan
Сетевой мост	bridge brx
Ethernet	ethernet ethx
Ethernet PPPoE	ethernet ethx pppoe номер
Виртуальный интерфейс Ethernet	ethernet ethx vif идентификатор_vlan
Ethernet Vif PPPoE	ethernet ethx vif идентификатор_vlan pppoe номер
Интерфейс заглушки	loopback lo
Многоканальная связь	multilink mlx
OpenVPN	openvpn vtunx
Псевдо-Ethernet	pseudo-ethernet pethx
Последовательный интерфейс	serial srx vif идентификатор_vlan
Туннель	tunnel tunx

Форма **set** этой команды используется для применения политики фильтрации ARP к интерфейсу.

Форма **delete** этой команды используется для удаления политики фильтрации ARP с интерфейса.

Форма **show** этой команды используется для отображения настройки политики фильтрации ARP на интерфейсе.

30.1.2 policy arp <имя_политики>

Определение имени политики фильтрации ARP.

Синтаксис

```
set policy arp <имя_политики>
delete policy arp <имя_политики>
show policy arp <имя_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
      arp имя_политики {
      }
}
```

Параметры

имя_политики

Имя политики фильтрации ARP.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет определить имя политики фильтрации ARP.

Форма **set** данной команды используется для определения имени политики.

Форма **delete** используется для удаления политики.

Форма **show** используется для отображения настроек политики фильтрации ARP.

30.1.3 policy arp <имя_политики> default-action <действие>

Определение для указанной политики фильтрации ARP.

Синтаксис

```
set policy arp <имя_политики> default-action <действие>
delete policy arp <имя_политики> default-action
show policy arp <имя_политики> default-action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   arp имя_политики {
      default-action действие
   }
}
```

Параметры

имя_политики

Имя политики фильтрации ARP.

действие

Действие, задаваемое указанной политикой по умолчанию. Допустимые значения:

drop: отбросить пакеты без уведомления клиента;

accept: передача пакетов в дальнейшую обработку.

Значение по умолчанию

По умолчанию пакеты отбрасываются без уведомления (drop).

Указания по использованию

Данная команда позволяет определить для указанной политики фильтрации ARP действие по умолчанию.

Форма **set** данной команды используется для указания действия по умолчанию для заданной политики.

Форма **delete** используется для восстановления настройки по умолчанию.

Форма **show** используется для отображения настройки.

30.1.4 policy arp <имя_политики> description <описание>

Создание текстового описания для указанной политики фильтрации ARP.

Синтаксис

```
set policy arp <имя_политики> description <описание>
delete policy arp <имя_политики> description
show policy arp <имя_политики> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   arp имя_политики {
      description описание
   }
}
```

Параметры

имя_политики

Имя политики фильтрации ARP.

описание

Текстовое описание политики. В том случае если описание содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для задания текстового описания для указанной политики.

Форма **delete** используется для удаления описания.

Форма **show** используется для отображения описания.

30.1.5 policy arp <имя_политики> rule <номер_правила>

Определение правила политики фильтрации ARP.

Синтаксис

```
set policy arp <имя_политики> rule <номер_правила>
delete policy arp <имя_политики> rule <номер_правила>
show policy arp <имя_политики> rule <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    arp имя_политики {
        rule номер_правила {
        }
    }
}
```

Параметры

имя_политики

Имя политики фильтрации ARP.

номер_правила

Номер правила политики фильтрации ARP. Значение должно лежать в диапазоне 1-65535.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет определить правило в политике фильтрации ARP.

Форма **set** данной команды используется для определения номера правила.

Форма **delete** используется для удаления правила.

Форма **show** используется для отображения конфигурации указанного правила политики фильтрации ARP.

30.1.6 policy arp <имя_политики> rule <номер_правила> action <действие>

Указание действия для правила политики фильтрации ARP.

Синтаксис

```
set policy arp <имя_политики> rule <номер_правила> action <действие>
delete policy arp <имя_политики> rule <номер_правила> action
show policy arp <имя_политики> rule <номер_правила> action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    arp имя_политики {
        rule номер_правила {
            action действие
        }
```

```
    }
}
```

Параметры

имя_политики

Имя политики фильтрации ARP.

номер_правила

Номер правила политики фильтрации ARP. Значение должно лежать в диапазоне 1-65535.

действие

Действие, задаваемое для указанного правила. Допустимые значения:

drop: отбросить пакеты без уведомления клиента;

accept: передача пакетов в дальнейшую обработку.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для указания действия для правила политики фильтрации ARP.

Форма **delete** используется для удаления связанного с правилом действия.

Форма **show** используется для отображения существующей настройки.

30.1.7 policy arp <имя_политики> rule <номер_правила> destination ip <ipv4-адрес>

Указание IP-адреса или подсети назначения для правила политики фильтрации ARP.

Синтаксис

```
set policy arp <имя_политики> rule <номер_правила> destination ip <ipv4-адрес>
delete policy arp <имя_политики> rule <номер_правила> destination ip
show policy arp <имя_политики> rule <номер_правила> destination ip
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    arp имя_политики {
        rule номер_правила {
            destination {
                ip ipv4-адрес
            }
        }
    }
}
```

Параметры

имя_политики

Имя политики фильтрации ARP.

номер_правила

Номер правила политики фильтрации ARP. Значение должно лежать в диапазоне 1-65535.

ipv4-адрес

IP-адрес или подсеть назначения пакета для правила политики фильтрации ARP. Допустимые для задания параметра форматы представлены в таблице ниже.

Таблица 252– Допустимые форматы задания параметра.

Значение	Описание
<x.x.x.x>	IPv4-адрес.
<x.x.x.x/x>	Подсеть адресов IPv4.
!<x.x.x.x>	Все адреса за исключением указанного.
!<x.x.x.x/x>	Все подсети за исключением указанной.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для указания IP-адреса получателя для правила политики фильтрации ARP.

Форма **delete** используется для удаления связанного с правилом IP-адреса получателя.

Форма **show** используется для отображения существующей настройки.

30.1.8 policy arp <имя_политики> rule <номер_правила> destination mac <mac-адрес>

Указание MAC-адреса назначения для правила политики фильтрации ARP.

Синтаксис

```
set policy arp <имя_политики> rule <номер_правила> destination mac <mac-адрес>
delete policy arp <имя_политики> rule <номер_правила> destination mac
show policy arp <имя_политики> rule <номер_правила> destination mac
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    arp имя_политики {
        rule номер_правила {
            destination {
                mac mac-адрес
            }
        }
    }
}
```

Параметры

имя_политики

Имя политики фильтрации ARP.

номер_правила

Номер правила политики фильтрации ARP. Значение должно лежать в диапазоне 1-65535.

mac-адрес

MAC-адрес назначения для правила политики фильтрации ARP. Допустимые для задания параметра форматы представлены в таблице ниже.

Таблица 253– Формат указания MAC-адреса

Значение	Описание
<h:h:h:h:h:h>	MAC-адрес.
!<h:h:h:h:h:h>	Все адреса за исключением указанного.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для указания MAC-адреса назначения для правила политики фильтрации ARP.

Форма **delete** используется для удаления связанного с правилом MAC-адреса назначения.

Форма **show** используется для отображения существующей настройки.

30.1.9 policy arp <имя_политики> rule <номер_правила> hardware-length <длина>

Указание длины физического адреса в байтах для правила политики фильтрации ARP.

Синтаксис

```
set policy arp <имя_политики> rule <номер_правила> hardware-length <длина>
delete policy arp <имя_политики> rule <номер_правила> hardware-length
show policy arp <имя_политики> rule <номер_правила>  hardware-length
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   arp имя_политики {
      rule номер_правила {
         hardware-length длина
      }
   }
}
```

Параметры

имя_политики

Имя политики фильтрации ARP.

номер_правила

Номер правила политики фильтрации ARP. Значение должно лежать в диапазоне 1-65535.

длина_адреса

Длина физического адреса в байтах. Например, адрес Ethernet имеет длину 6 байт. Значения должны лежать в диапазоне 1-255.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для указания длины физического адреса для правила политики фильтрации ARP.

Форма **delete** используется для удаления связанного с правилом значения длины физического адреса.

Форма **show** используется для отображения существующей настройки.

30.1.10 policy arp <имя_политики> rule <номер_правила> hardware-type <протокол>

Указание протокола канального уровня для правила политики фильтрации ARP.

Синтаксис

```
set policy arp <имя_политики> rule <номер_правила> hardware-type <протокол>
delete policy arp <имя_политики> rule <номер_правила> hardware-type
show policy arp <имя_политики> rule <номер_правила>  hardware- type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   arp имя_политики {
      rule номер_правила {
         hardware-type протокол
      }
   }
}
```

Параметры

имя_политики

Имя политики фильтрации ARP.

номер_правила

Номер правила политики фильтрации ARP. Значение должно лежать в диапазоне 1-65535.

протокол

Протокол канального уровня. Допустимые значение представлены в таблице ниже.

Таблица 254– Формат указания протокола

Значение	Описание
<ethernet>	название протокола (для Ethernet).
<1-ffff>	Номер протокола в шестнадцатеричном формате.
<1-ffff/1-ffff>	Номер протокола с маской в шестнадцатеричном формате.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для указания *протокола канального уровня* для правила политики фильтрации ARP.

Форма **delete** используется для удаления существующей *настройки*.

Форма **show** используется для отображения существующей настройки.

30.1.11 policy arp <имя_политики> rule <номер_правила> operation <код_операции>

Указание кода операции для правила политики фильтрации ARP.

Синтаксис

```
set policy arp <имя_политики> rule номер_правила operation <код_операции>
delete policy arp <имя_политики> rule <номер_правила> operation
```

```
show policy arp <имя_политики> rule <номер_правила> operation
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   arp имя_политики {
      rule номер_правила {
         operation код_операции
      }
   }
}
```

Параметры

имя_политики

Имя политики фильтрации ARP.

номер_правила

Номер правила политики фильтрации ARP. Значение должно лежать в диапазоне 1-65535.

код_операции

Код операции. Допустимые форматы задания значения представлены в таблице ниже.

Таблица 255– Формат указания кода операции

Значение	Описание
<1-ffff>	Код операции в шестнадцатеричном формате.
<1-ffff/1-ffff>	Код операции с маской в шестнадцатеричном формате.
1	Request.
2	Reply.
3	Request_Reverse.
4	Reply_Reverse.
5	DRARP_Request.
6	DRARP_Reply.
7	DRARP_Error.
8	InARP_Request.
9	InARP_Reply.
A	ARP_NAK.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для указания кода операции для правила политики фильтрации ARP.

Форма **delete** используется для удаления связанного с правилом значения кода операции.

Форма **show** используется для отображения существующей настройки.

30.1.12 policy arp <имя_политики> rule <номер_правила> source ip <ipv4-адрес>

Указание IP-адреса или подсети источника (отправителя) для правила политики фильтрации ARP.

Синтаксис

```
set policy arp <имя_политики> rule <номер_правила> source ip <ipv4-адрес>
```

```
delete policy arp <имя_политики> rule <номер_правила> source ip
show policy arp <имя_политики> rule <номер_правила> source ip
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   arp имя_политики {
      rule номер_правила {
         source {
            ip ipv4-адрес
         }
      }
   }
}
```

Параметры

имя_политики

Имя политики фильтрации ARP.

номер_правила

Номер правила политики фильтрации ARP. Значение должно лежать в диапазоне 1-65535.

ipv4-адрес

IP-адрес или подсеть источника (отправителя) для правила политики фильтрации ARP. Допустимые для задания параметра форматы представлены в таблице ниже.

Таблица 256– Допустимые форматы задания параметра.

Значение	Описание
<x.x.x.x>	IPv4-адрес.
<x.x.x.x/x>	Подсеть адресов IPv4.
!<x.x.x.x>	Все адреса за исключением указанного.
!<x.x.x.x/x>	Все подсети за исключением указанной.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для указания IP-адреса или подсети источника (отправителя) для правила политики фильтрации ARP.

Форма **delete** используется для удаления связанного с правилом IP-адреса или подсети источника.

Форма **show** используется для отображения существующей настройки.

30.1.13 policy arp <имя_политики> rule <номер_правила> source mac <mac-адрес>

Указание MAC-адреса источника (отправителя) для правила политики фильтрации ARP.

Синтаксис

```
set policy arp <имя_политики> rule <номер_правила> source mac <mac-адрес>
delete policy arp <имя_политики> rule <номер_правила> source mac
show policy arp <имя_политики> rule <номер_правила> source mac
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   arp имя_политики {
      rule номер_правила {
         source {
            mac mac-адрес
         }
      }
   }
}
```

Параметры

имя_политики

Имя политики фильтрации ARP.

номер_правила

Номер правила политики фильтрации ARP. Значение должно лежать в диапазоне 1-65535.

mac-адрес

MAC-адрес источника (отправителя) для правила политики фильтрации ARP. Допустимые для задания параметра форматы представлены в таблице ниже.

Таблица 257– Формат указания MAC-адреса

Значение	Описание
<h:h:h:h:h:h>	MAC-адрес.
!<h:h:h:h:h:h>	Все адреса за исключением указанного.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для указания MAC-адреса источника (отправителя) для правила политики фильтрации ARP.

Форма **delete** используется для удаления связанного с правилом MAC-адреса источника.

Форма **show** используется для отображения существующей настройки.

30.1.14 policy arp <имя_политики> rule <номер_правила> protocol-type <протокол>

Указание протокола сетевого уровня для правила политики фильтрации ARP.

Синтаксис

```
set policy arp <имя_политики> rule <номер_правила> protocol-type <протокол>
delete policy arp <имя_политики> rule <номер_правила> protocol-type
show policy arp <имя_политики> rule <номер_правила>  protocol- type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   arp имя_политики {
```

```
        rule номер_правила {
            protocol-type протокол
        }
    }
}
```

Параметры

имя_политики

Имя политики фильтрации ARP.

номер_правила

Номер правила политики фильтрации ARP. Значение должно лежать в диапазоне 1-65535.

протокол

Протокол сетевого уровня. Допустимые значение представлены в таблице ниже.

Таблица 258– Формат указания протокола

Значение	Описание
<ipv4>	название протокола (для IPv4).
<1-ffff>	Номер протокола в шестнадцатеричном формате.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для указания протокола сетевого уровня для правила политики фильтрации ARP.

Форма **delete** используется для удаления существующей настройки.

Форма **show** используется для отображения существующей настройки.

30.1.15 policy clear arp <имя_политики>

Очистка статистики политики фильтрации ARP.

Синтаксис

```
policy clear arp <имя_политики>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики фильтрации ARP.

Значение по умолчанию

Отсутствует.

30.1.16 policy show arp <имя_политики>

Вывод сведений и статистики для указанной политики фильтрации ARP.

Синтаксис

```
policy show arp <имя_политики> [detail]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики фильтрации ARP.

detail

Вывод подробных сведений по указанной политике.

Значение по умолчанию

Отсутствует.

Примеры

В примере ниже приведен образец работы команды вывода конфигурации политики фильтрации ARP.

Пример 302 - Вывод конфигурации политики фильтрации ARP.

```
admin@edge:~$ policy show arp test
Политика фильтрации ARP test:

 Политика не задействована ни для одного интерфейса, туннеля или зоны.


rule      target    src MAC             dst MAC
----      ------    -------             -------
10        ACCEPT    *                   *
default   DROP      *                   *
```

В примере ниже приведен образец работы команды вывода подробной конфигурации политики фильтрации ARP.

Пример 303 - Вывод подробной конфигурации политики фильтрации ARP.

```
admin@edge:~$ policy show arp test detail
Политика фильтрации ARP test:

 Политика не задействована ни для одного интерфейса, туннеля или зоны.


rule      pkts      bytes     target    src MAC             dst MAC
----      ----      -----     ------    -------             -------
10        0         0         ACCEPT    *                   *
    -d 192.168.10.150 --opcode 2 --h-type 1
default   0         0         DROP      *                   *
```

30.1.17 policy show arp <имя_политики> rule <номер_правила>

Вывод конфигурации для правила политики фильтрации ARP.

Синтаксис

```
policy show arp <имя_политики> rule <номер_правила> [detail]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики фильтрации ARP.

номер_правила

Номер правила политики фильтрации ARP. Значение должно лежать в диапазоне 1-65535.

detail

Вывод подробных сведений по указанному правилу политики.

Значение по умолчанию

Отсутствует.

31 Политика фильтрации на канальном уровне

В данном разделе представлены сведения о средствах фильтрации трафика на канальном уровне в Numa Edge.

31.1 Команды настройки политик фильтрации трафика на канальном уровне

В данном разделе приведены команды для настройки политик фильтрации трафика на канальном уровне.

Режим настройки	
interfaces <интерфейс> policy <направление> ethernet <имя_политики>	Применение политики фильтрации на канальном уровне к указанному интерфейсу
policy ethernet <имя_политики>	Определение имени политики маршрутизации трафика.
policy ethernet <имя_политики> default-action <действие>	Определение для указанной политики фильтрации трафика на канальном уровне действия по умолчанию.
policy ethernet <имя_политики> description <описание>	Указание краткого описания для политики фильтрации на канальном уровне.
policy ethernet <имя_политики> enable-default-log	Включение/отключение для указанной политики фильтрации трафика на канальном уровне протоколирования действия по умолчанию.
policy ethernet <имя_политики> rule <номер_правила>	Определение правила политики фильтрации на канальном уровне.
policy ethernet <имя> rule <номер_правила> action <действие>	Указание действия, которое будет применяться к пакетам, для которых было установлено соответствие правилу.
policy ethernet <имя_политики> rule <номер_правила> description <описание>	Указание краткого описания для указанного правила политики фильтрации на канальном уровне.
policy ethernet <имя_политики> rule <номер_правила> destination mac <mac-адрес>	Указание MAC-адреса назначения для правила политики фильтрации на канальном уровне.
policy ethernet <имя_политики> rule <номер_правила> disable	Отключение/включение правила политики фильтрации на канальном уровне.
policy ethernet <имя_политики> rule <номер_правила> ethertype <протокол>	Задание для указанного правила протокола, с которым будет сверяться протокол, пакет которого инкапсулирован в проверяемом Ethernet-кадре.
policy ethernet <имя_политики> rule <номер_правила> log <состояние>	Включение/выключение регистрации событий фильтрации трафика на канальном уровне для указанного правила указанной политики.
policy ethernet <имя_политики> rule <номер_правила> source mac <mac-адрес>	Указание MAC-адреса источника (отправителя).
policy ethernet <имя_политики> rule <номер_правила> vlan id <идентификатор_vlan>	Задание идентификатора VLAN.
policy ethernet <имя_политики> rule <номер_правила> vlan ethertype <протокол>	Задание для указанного правила протокола VLAN.
policy ethernet <имя_политики> rule <номер_правила> vlan prio <приоритет>	Назначение приоритета vlan для указанного правила политики.
Эксплуатационный режим	
policy clear ethernet <имя_политики>	Очистка конфигурации политики фильтрации на канальном уровне.
policy clear ethernet <имя_политики> rule <номер_правила>	Очистка конфигурации указанного правила политики фильтрации на канальном уровне.
policy show ethernet <имя_политики>	Очистка конфигурации политики фильтрации на канальном уровне.
policy show ethernet <имя_политики> rule <номер_правила>	Очистка конфигурации указанного правила политики фильтрации на канальном уровне.

31.1.1 interfaces <интерфейс> policy <направление> ethernet <имя_политики>

Применение политики фильтрации на канальном уровне к указанному интерфейсу.

Синтаксис

```
set interfaces <интерфейс> policy <направление> ethernet <имя_политики>
delete interfaces <интерфейс> policy <направление> Ethernet
show interfaces <интерфейс> policy <направление> ethernet
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
   policy {
      направление {
         ethernet имя_политики      }
   }
}
```

Параметры

интерфейс

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже в разделе Указания по использованию.

направление

Обязательный. Направление трафика, к которому применяется политика фильтрации на канальном уровне. Допустимые значения указаны в таблице ниже:

Таблица 259 – Направления трафика

Значение	Описание
in	Транзитный трафик, принимаемый на указанном интерфейсе
out	Транзитный трафик, отправляемый с указанного интерфейса
local	Трафик, принятый на интерфейсе, предназначенный для локальной системы.

имя_политики

Имя политики фильтрации на канальном уровне, применяемой к данному интерфейсу.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для применения политики фильтрации на канальном уровне к интерфейсу.

Фильтрация транзитного трафика или трафика, предназначенного для локальной системы, не осуществляется до тех пор, пока политика межсетевого экранирования не будет применена к интерфейсу (реальному или виртуальному) с использованием данной команды.

На каждом интерфейсе можно применить до трех политик межсетевого экранирования: одну как фильтр транзитного трафика, принимаемого на интерфейсе (in), одну – как фильтр транзитного трафика, покидающего интерфейс (out) и одну – как фильтр трафика, предназначенного для локальной системы (local).

В приведенной ниже таблице показаны типы поддерживаемых интерфейсов и синтаксис.

Таблица 260 – Типы интерфейсов

Тип интерфейса	Синтаксис
Агрегирование каналов	bonding bondx

Виртуальный интерфейс агрегированных каналов	bonding bondx vif идентификатор_vlan
Сетевой мост	bridge brx
Ethernet	ethernet ethx
Ethernet PPPoE	ethernet ethx pppoe номер
Виртуальный интерфейс Ethernet	ethernet ethx vif идентификатор_vlan
Ethernet Vif PPPoE	ethernet ethx vif идентификатор_vlan pppoe номер
Интерфейс заглушки	loopback lo
Многоканальная связь	multilink mlx
OpenVPN	openvpn vtunx
Псевдо-Ethernet	pseudo-ethernet pethx
Последовательный интерфейс	serial srx vif идентификатор_vlan
Туннель	tunnel tunx

Форма **set** этой команды используется для применения политики фильтрации на канальном уровне к интерфейсу.

Форма **delete** этой команды используется для удаления политики фильтрации на канальном уровне с интерфейса.

Форма **show** этой команды используется для отображения настройки политики фильтрации на канальном уровне на интерфейсе.

31.1.2 policy ethernet <имя_политики>

Определение имени политики маршрутизации трафика.

Синтаксис

```
set policy ethernet <имя_политики>
delete policy ethernet <имя_политики>
show policy ethernet <имя_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    ethernet имя_политики {
    }
}
```

Параметры

имя_политики

Имя политики фильтрации трафика на канальном уровне.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет определить имя политики фильтрации трафика на канальном уровне.

Форма **set** данной команды используется для определения имени политики.

Форма **delete** используется для удаления политики.

Форма **show** используется для отображения настроек политики фильтрации трафика на канальном уровне.

31.1.3 policy ethernet <имя_политики> default-action <действие>

Определение для указанной политики фильтрации трафика на канальном уровне действия по умолчанию.

Синтаксис

```
set policy ethernet <имя_политики> default-action <действие>
delete policy ethernet <имя_политики> default-action
show policy ethernet <имя_политики> default-action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    ethernet имя_политики {
        default-action действие
    }
}
```

Параметры

имя_политики

Имя политики фильтрации трафика на канальном уровне.

действие

Действие, задаваемое указанной политикой по умолчанию. Допустимые значения:

drop: отбросить кадры без уведомления клиента;

accept: передача кадров в дальнейшую обработку.

Значение по умолчанию

По умолчанию кадры отбрасываются (drop).

Указания по использованию

Данная команда позволяет определить для указанной политики фильтрации трафика на канальном уровне действия по умолчанию.

Форма **set** данной команды используется для указания действия по умолчанию для заданной политики.

Форма **delete** используется для удаления настройки.

Форма **show** используется для отображения настройки.

31.1.4 policy ethernet <имя_политики> description <описание>

Указание краткого описания для политики фильтрации на канальном уровне.

Синтаксис

```
set policy ethernet <имя_политики> description <описание>
delete policy ethernet <имя_политики> description
show policy ethernet <имя_политики> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    ethernet имя_политики {
        description описание
    }
}
```

Параметры

имя_политики

Имя политики фильтрации трафика на канальном уровне.

описание

Описание политики фильтрации трафика на канальном уровне. В том случае если описание содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать описание для политики фильтрации на канальном уровне.

Форма **set** данной команды используется для создания и изменения описания.

Форма **delete** используется для удаления описания.

Форма **show** используется для отображения настройки описания.

31.1.5 policy ethernet <имя_политики> enable-default-log

Включение/отключение для указанной политики фильтрации трафика на канальном уровне протоколирования действия по умолчанию.

Синтаксис

```
set policy ethernet <имя_политики> enable-default-log
delete policy ethernet <имя_политики> enable-default-log
show policy ethernet <имя_политики> enable-default-log
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   ethernet имя_политики {
      enable-default-log
   }
}
```

Параметры

имя_политики

Имя политики фильтрации трафика на канальном уровне.

Значение по умолчанию

Не установлено.

Указания по использованию

Данная команда позволяет включить для указанной политики фильтрации трафика на канальном уровне протоколирование действия по умолчанию.

Форма **set** данной команды используется для включения протоколирования.

Форма **delete** используется для отключения протоколирования.

Форма **show** используется для отображения текущей настройки протоколирования.

31.1.6 policy ethernet <имя_политики> rule <номер_правила>

Определение правила политики фильтрации на канальном уровне.

Синтаксис

```
set policy ethernet <имя_политики> rule <номер_правила>
delete policy ethernet <имя_политики> rule <номер_правила>
show policy ethernet <имя_политики> rule <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    ethernet имя_политики {
        rule номер_правила {
        }
    }
}
```

Параметры

имя_политики

Имя политики фильтрации на канальном уровне.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет определить правило в политике фильтрации на канальном уровне.

Форма **set** данной команды используется для определения номера правила.

Форма **delete** используется для удаления правила.

Форма **show** используется для отображения конфигурации указанного правила политики фильтрации трафика на канальном уровне.

31.1.7 policy ethernet <имя> rule <номер_правила> action <действие>

Указание действия, которое будет применяться к пакетам, для которых было установлено соответствие правилу.

Синтаксис

```
set policy ethernet <имя_политики> rule <номер_правила> action <действие>
delete policy ethernet <имя_политики> rule <номер_правила> action
show policy ethernet <имя_политики> rule <номер_правила> action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy{
    ethernet имя_политики {
        rule номер_правила {
            action действие
```

```
        }
    }
}
```

Параметры

имя_политики

Имя политики фильтрации на канальном уровне.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

действие

Действие, которое будет выполнено, в том случае если кадр удовлетворяет критериям, указанным в правиле. Поддерживаются следующие значения:

accept: Принять и переслать кадр, для которого было установлено соответствие, в дальнейшую обработку.

drop: Отбросить кадр, для которого было установлено соответствие.

exlude: Исключение трафика. Вызывает выполнение действия, указанного как default-action командой **policy ethernet <имя_политики> default-action <действие>**.

Значение по умолчанию

По умолчанию кадры отбрасываются (drop).

Указания по использованию

Данная команда позволяет указать действие, которое будет применено к кадрам, для которых было установлено соответствие критериям, указанным в правиле.

В правиле может быть указано только одно действие.

Форма **set** данной команды используется для указания действия, которое будет применяться к пакетам, для которых установлено соответствие критериям правила.

Форма **delete** данной команды позволяет восстановить действие, принятое по умолчанию.

Форма **show** данной команды используется для отображения настройки действия для правила политики фильтрации на канальном уровне.

31.1.8 policy ethernet <имя_политики> rule <номер_правила> description <описание>

Указание краткого описания для указанного правила политики фильтрации на канальном уровне.

Синтаксис

```
set policy ethernet <имя_политики> rule <номер_правила> description <описание>
delete policy ethernet <имя_политики> rule <номер_правила> description
show policy ethernet <имя_политики> rule <номер_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    ethernet имя_политики {
        rule номер_правила {
            description описание
        }
```

```
    }
}
```

Параметры

имя_политики

Имя политики фильтрации трафика на канальном уровне.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

описание

Описание политики фильтрации трафика на канальном уровне. В том случае если описание содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать описание для указанного правила политики фильтрации на канальном уровне.

Форма **set** данной команды используется для создания и изменения описания.

Форма **delete** используется для удаления описания.

Форма **show** используется для отображения описания.

31.1.9 policy ethernet <имя_политики> rule <номер_правила> destination mac <mac-адрес>

Указание MAC-адреса назначения для правила политики фильтрации на канальном уровне.

Синтаксис

```
set policy ethernet <имя_политики> rule <номер_правила> destination mac <mac-адрес>
delete policy ethernet <имя_политики> rule <номер_правила> destination mac
show policy ethernet <имя_политики> rule <номер_правила> destination mac
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    ethernet имя_политики {
        rule номер_правила {
            destination {
                mac mac-адрес
            }
        }
    }
}
```

Параметры

имя_политики

Имя политики фильтрации трафика на канальном уровне.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

mac-адрес

MAC-адрес назначения для правила политики фильтрации на канальном уровне. Допустимые для задания параметра форматы представлены в таблице ниже.

Таблица 261 – Форматы указания MAC-адреса

Значение	Описание
<h:h:h:h:h:h>	MAC-адрес
!<h:h:h:h:h:h>	Все адреса за исключением указанного
<h:h:h:h:h:h>/<h:h:h:h:h:h>	Множество адресов, задаваемое адресом и маской
!<h:h:h:h:h:h>/<h:h:h:h:h:h>	Все адреса, кроме указанного множества
Unicast	соответствует однонаправленным адресам 00:00:00:00:00:00/01:00:00:00:00:00
multicast	соответствует мультивещательным адресам 01:00:00:00:00:00/01:00:00:00:00:00
broadcast	соответствует широковещательному адресу ff:ff:ff:ff:ff:ff
Bga	соответствует bridge group адресу 01:80:c2:00:00:00/ff:ff:ff:ff:ff:ff

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для указания MAC-адреса назначения для правила политики фильтрации на канальном уровне.

Форма **delete** используется для удаления связанного с правилом MAC-адреса назначения.

Форма **show** используется для отображения существующей настройки.

31.1.10 policy ethernet <имя_политики> rule <номер_правила> disable

Отключение/включение правила политики фильтрации на канальном уровне.

Синтаксис

```
set policy ethernet <имя_политики> rule <номер_правила> disable
delete policy ethernet <имя_политики> rule <номер_правила> disable
show policy ethernet <имя_политики> rule <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    ethernet имя_политики {
        rule номер_правила {
            disable
        }
    }
}
```

Параметры

имя_политики

Имя политики фильтрации трафика на канальном уровне.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет отключить правило без удаления соответствующего узла конфигурации.

Форма **set** данной команды позволяет отключить указанное правило политики фильтрации на канальном уровне.

Форма **delete** используется для включения ранее отключенного правила.

Форма **show** используется для отображения текущей настройки правила политики.

31.1.11 policy ethernet <имя_политики> rule <номер_правила> ethertype <протокол>

Задание для указанного правила протокола, с которым будет сверяться протокол, пакет которого инкапсулирован в проверяемом Ethernet-кадре.

Синтаксис

```
set policy ethernet <имя_политики> rule <номер_правила> ethertype <протокол>
delete policy ethernet <имя_политики> rule <номер_правила> ethertype [протокол]
show policy ethernet <имя_политики> rule <номер_правила> ethertype
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    ethernet имя_политики {
        rule номер_правила {
            ethertype протокол
        }
    }
}
```

Параметры

имя_политики

Имя политики фильтрации трафика на канальном уровне.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

протокол

Протокол, пакет которого инкапсулирован в Ethernet-кадре. Допустимые форматы значений представлены в таблице ниже.

Таблица 262 – Формат указания протокола

Значение	**Описание**
<600-ffff>	Номер протокола в шестнадцатеричном формате
!<600-ffff>	Все кадры за исключением кадров с указанным протоколом
ipv4	IPv4
x.25	X.25
Arp	Address Resolution Protocol
frame-relay-arp	Frame Relay ARP
Bpq	G8BPQ AX.25 Ethernet
Dec	DEC Assigned protocol
dec-dna-dl	DEC DNA Dump/Load
dec-dna-rc	DEC DNA Remote Console
dec-dna-re	DEC DNA Routing
dec-lat	DEC LAT
dec-diag	DEC Diagnostics
dec-cust	DEC Customer use
dec-sca	DEC Systems Comms Arch
Teb	Trans Ether Bridging
frame-relay-raw	Raw Frame Relay
Aarp	Appletalk AARP
Appletalk	Appletalk DDP
802.1q	802.1Q Virtual LAN tagged frame
Ipx	Novell IPX
Netbeui	NetBIOS Extended User Interface
ipv6	IPv6
Ppp	Point-to-Point Protocol
atm-mpoa	MultiProtocol Over ATM
pppoe-disc	PPPoE discovery messages
pppoe-ses	PPPoE session messages
atm-fate	Frame-based ATM Transport over Ethernet
Loop	Ethernet Loopback protocol
Length	Номер протокола меньше 0x600 и используется в качестве длины

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для задания протокола для сравнения для указанного правила.

Форма **delete** этой команды используется для удаления ассоциированного с правилом протокола.

Форма **show** этой команды используется для отображения установленной настройки.

31.1.12 policy ethernet <имя_политики> rule <номер_правила> log <состояние>

Включение/выключение регистрации событий фильтрации трафика на канальном уровне для указанного правила указанной политики.

Синтаксис

```
set policy ethernet <имя_политики> rule <номер_правила> log <состояние>
```

```
delete policy ethernet <имя_политики> rule <номер_правила> log
show policy ethernet <имя_политики> rule <номер_правила> log
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    ethernet имя_политики {
        rule номер_правила {
            log состояние
        }
    }
}
```

Параметры

имя_политики

Имя политики фильтрации трафика на канальном уровне.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

состояние

Указывает параметры регистрации событий для правила политики. Допустимые значения:

enable: включить регистрацию;

disable: отключить регистрацию.

Значение по умолчанию

Отсутствует.

Указания по использованию

В том случае, если задействовано журналирование для правила политики, в системный лог (журнал) будут выводиться сообщения для всех пакетов, подпадающих под правило. Для каждого сообщения формируется префикс в квадратных скобках ([e-<имя>-<номер правила>-<действие>]). Имя политики может быть записано в журнале не полностью в связи с системным ограничением общей длины префикса в 29 символов.

Форма **set** этой команды используется для задания настройки регистрации событий фильтрации для указанного правила указанной политики.

Форма **delete** этой команды используется для удаления настройки регистрации событий фильтрации.

Форма **show** этой команды используется для отображения настройки регистрации событий фильтрации.

31.1.13 policy ethernet <имя_политики> rule <номер_правила> source mac <mac-адрес>

Указание MAC-адреса источника (отправителя).

Синтаксис

```
set policy ethernet <имя_политики> rule <номер_правила> source mac <mac-адрес>
delete policy ethernet <имя_политики> rule <номер_правила> source mac
show policy ethernet <имя_политики> rule <номер_правила> source mac
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   ethernet имя_политики {
      rule номер_правила {
         source {
            mac mac-адрес
         }
      }
   }
}
```

Параметры

имя_политики

Имя политики фильтрации трафика на канальном уровне.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

mac-адрес

MAC-адрес назначения для правила политики фильтрации на канальном уровне. Допустимые для задания параметра форматы представлены в таблице ниже.

Таблица 263 – Форматы указания MAC-адреса

Значение	Описание
<h:h:h:h:h:h>	MAC-адрес
!<h:h:h:h:h:h>	Все адреса за исключением указанного
<h:h:h:h:h:h>/<h:h:h:h:h:h>	Множество адресов, задаваемое адресом и маской
!<h:h:h:h:h:h>/<h:h:h:h:h:h>	Все адреса, кроме указанного множества
Unicast	соответствует однонаправленным адресам 00:00:00:00:00:00/01:00:00:00:00:00
Multicast	соответствует мультивещательным адресам 01:00:00:00:00:00/01:00:00:00:00:00
Broadcast	соответствует широковещательному адресу ff:ff:ff:ff:ff:ff
Bga	соответствует bridge group адресу 01:80:c2:00:00:00/ff:ff:ff:ff:ff:ff

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для указания MAC-адреса источника для правила политики фильтрации на канальном уровне.

Форма **delete** используется для удаления связанного с правилом MAC-адреса источника.

Форма **show** используется для отображения существующей настройки.

31.1.14 policy ethernet <имя_политики> rule <номер_правила> vlan id <идентификатор_vlan>

Задание идентификатора VLAN.

Синтаксис

```
set policy ethernet <имя_политики> rule <номер_правила> vlan id <идентификатор_vlan>
delete policy ethernet <имя_политики> rule <номер_правила> vlan id
show policy ethernet <имя_политики> rule <номер_правила> vlan id
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    ethernet имя_политики {
        rule номер_правила {
            vlan {
                id идентификатор_vlan
            }
        }
    }
}
```

Параметры

имя_политики

Имя политики фильтрации трафика на канальном уровне.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

идентификатор_vlan

Идентификатор VLAN. Допустимые значения:

<0-4095>: Идентификатор VLAN;

!<0-4095>: Всё, за исключением кадров с указанным идентификатором.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для установления соответствия кадрам с указанным идентификатором vlan для правила политики фильтрации трафика на канальном уровне.

ПРИМЕЧАНИЕ Для того чтобы задать конфигурацию данной командой, необходимо, чтобы протокол, указываемый командой **policy ethernet <имя_политики> rule <номер_правила> ethertype <протокол>** был 802.1q.

Форма **set** данной команды используется для указания идентификатора vlan для правила политики фильтрации на канальном уровне.

Форма **delete** используется для удаления связанного с правилом идентификатора vlan.

Форма **show** используется для отображения существующей настройки.

31.1.15 policy ethernet <имя_политики> rule <номер_правила> vlan ethertype <протокол>

Задание для указанного правила протокола VLAN.

Синтаксис

```
set policy ethernet <имя_политики> rule <номер_правила> vlan ethertype <протокол>
delete policy ethernet <имя_политики> rule <номер_правила> vlan ethertype
show policy ethernet <имя_политики> rule <номер_правила> vlan ethertype
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    ethernet имя_политики {
        rule номер_правила {
            vlan {
                ethertype протокол
            }
        }
    }
}
```

Параметры

имя_политики

Имя политики фильтрации трафика на канальном уровне.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

протокол

Протокол, пакет которого инкапсулирован в Ethernet-кадре. Допустимые форматы значений представлены в таблице ниже.

Таблица 264 – Формат указания протокола

Значение	Описание
<600-ffff>	Номер протокола в шестнадцатеричном формате
!<600-ffff>	Все кадры за исключением кадров с указанным протоколом
ipv4	IPv4
x.25	X.25
Arp	Address Resolution Protocol
frame-relay-arp	Frame Relay ARP
Bpq	G8BPQ AX.25 Ethernet
Dec	DEC Assigned protocol
dec-dna-dl	DEC DNA Dump/Load
dec-dna-rc	DEC DNA Remote Console
dec-dna-re	DEC DNA Routing

Значение	Описание
dec-lat	DEC LAT
dec-diag	DEC Diagnostics
dec-cust	DEC Customer use
dec-sca	DEC Systems Comms Arch
Teb	Trans Ether Bridging
frame-relay-raw	Raw Frame Relay
Aarp	Appletalk AARP
Appletalk	Appletalk DDP
802.1q	802.1Q Virtual LAN tagged frame
Ipx	Novell IPX
Netbeui	NetBIOS Extended User Interface
ipv6	IPv6
Ppp	Point-to-Point Protocol
atm-mpoa	MultiProtocol Over ATM
pppoe-disc	PPPoE discovery messages
pppoe-ses	PPPoE session messages
atm-fate	Frame-based ATM Transport over Ethernet
Loop	Ethernet Loopback protocol
Length	Номер протокола меньше 0x600 и используется в качестве длины

Значение по умолчанию

Отсутствует.

Указания по использованию

ПРИМЕЧАНИЕ Для того чтобы задать конфигурацию данной командой, необходимо, чтобы протокол, указываемый командой **policy ethernet <имя_политики> rule <номер_правила> ethertype <протокол>** был 802.1q.

Форма **set** этой команды используется для задания для указанного правила протокола (или группы протоколов) VLAN.

Форма **delete** этой команды используется для удаления ассоциированного с правилом протокола VLAN.

Форма **show** этой команды используется для отображения установленной настройки.

31.1.16 policy ethernet <имя_политики> rule <номер_правила> vlan prio <приоритет>

Назначение приоритета vlan для указанного правила политики.

Синтаксис

```
set policy ethernet <имя_политики> rule <номер_правила> vlan prio <приоритет>
delete policy ethernet <имя_политики> rule <номер_правила> vlan prio
show policy ethernet <имя_политики> rule <номер_правила> vlan prio
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   ethernet имя_политики {
      rule номер_правила {
         vlan {
            ethertype протокол
```

```
            }
        }
    }
}
```

Параметры

имя_политики

Имя политики фильтрации трафика на канальном уровне.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

приоритет

Значение приоритета vlan. Допустимые значения:

<0-7>: приоритет;

!<0-7>: все кадры, за исключением кадров с указанным приоритетом.

Значение по умолчанию

Отсутствует.

Указания по использованию

ПРИМЕЧАНИЕ Для того чтобы задать конфигурацию данной командой, необходимо, чтобы протокол, указываемый командой **policy ethernet <имя_политики> rule <номер_правила> ethertype <протокол>** был 802.1q.

Форма **set** этой команды используется для задания для указанного правила приоритета vlan.

Форма **delete** этой команды используется для удаления заданного в правиле приоритета vlan.

Форма **show** этой команды используется для отображения установленной настройки.

31.1.17 policy clear ethernet <имя_политики>

Очистка статистики для указанной политики фильтрации на канальном уровне.

Синтаксис

```
clear policy ethernet <имя_политики>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики фильтрации трафика на канальном уровне.

Значение по умолчанию

Отсутствует.

31.1.18 policy clear ethernet <имя_политики> rule <номер_правила>

Очистка статистики правила политики фильтрации на канальном уровне.

Синтаксис

```
policy clear ethernet <имя_политики> rule <номер_правила>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики фильтрации трафика на канальном уровне.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

Значение по умолчанию

Отсутствует.

31.1.19 policy show ethernet <имя_политики>

Отображение конфигурации политики фильтрации на канальном уровне.

Синтаксис

```
policy show ethernet <имя_политики> [detail]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики фильтрации трафика на канальном уровне.

detail

Отображение подробных сведений об указанной политике фильтрации на канальном уровне.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения сведений о выбранной настроенной политике фильтрации на канальном уровне.

Примеры

В примере ниже приведен образец работы команды вывода конфигурации политики фильтрации на канальном уровне.

Пример 304 - Вывод конфигурации политики фильтрации на канальном уровне.

```
admin@edge:~$ policy show ethernet test
Политика фильтрации Ethernet test:

 Политика не задействована ни для одного интерфейса, туннеля или зоны.


rule      target    src MAC             dst MAC
----      ------    -------             -------
10        ACCEPT    *                   *
20        DROP      broadcast           *
default   DROP      *                   *
```

В примере ниже приведен образец работы команды подробного вывода конфигурации политики фильтрации на канальном уровне (с указанием ключевого слова **detail**).

Пример 305 - Вывод подробной конфигурации политики фильтрации на канальном уровне.

```
admin@edge:~$ policy show ethernet test detail
Политика фильтрации Ethernet test:

 Политика не задействована ни для одного интерфейса, туннеля или зоны.


rule      pkts      bytes     target    src MAC             dst MAC
----      ----      -----     ------    -------             -------
10        0         0         ACCEPT    *                   *
    -p 802_1Q --vlan-id 15 --log-level notice --log-prefix "[e-test-10-AC] "
20        0         0         ACCEPT    broadcast           *
    -p IPv4 -s Broadcast
default   0         0         DROP      *                   *
```

31.1.20 policy show ethernet <имя_политики> rule <номер_правила>

Вывод конфигурации правила политики фильтрации на канальном уровне.

Синтаксис

```
show policy ethernet <имя_политики> rule <номер_правила> [detail]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики фильтрации трафика на канальном уровне.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

detail

Отображение подробных сведений об указанном правиле политики фильтрации на канальном уровне.

Значение по умолчанию

Отсутствует.

Примеры

В примере ниже приведен образец вывода конфигурации отдельного правила политики фильтрации на канальном уровне.

Пример 306 - Вывод конфигурации отдельного правила политики фильтрации на канальном уровне.

```
admin@edge:~$ policy show ethernet test rule 10
Политика фильтрации Ethernet test:

 Политика не задействована ни для одного интерфейса, туннеля или зоны.


rule      target    src MAC             dst MAC
----      ------    -------             -------
10        ACCEPT    *                   *
```

В примере ниже приведен образец подробного вывода конфигурации отдельного правила политики фильтрации на канальном уровне (с указанием ключевого слова **detail**).

Пример 307 - Вывод подробной конфигурации отдельного правила политики фильтрации на канальном уровне.

```
admin@edge:~$ policy show ethernet test rule 10 detail
Политика фильтрации Ethernet test:

 Политика не задействована ни для одного интерфейса, туннеля или зоны.


rule      pkts      bytes     target    src MAC             dst MAC
----      ----      -----     ------    -------             -------
10        0         0         ACCEPT    *                   *
    -p 802_1Q --vlan-id 15 --log-level notice --log-prefix "[e-test-10-AC] "
```

32 Политика маршрутизации трафика

В этом разделе даны указания по настройке политик маршрутизации трафика на системе Numa Edge.

Рассматриваются следующие вопросы:

- Обзор политик маршрутизации трафика.
- Примеры настройки политик маршрутизации трафика.
- Команды политик маршрутизации трафика.

32.1 Обзор политик маршрутизации трафика

В обычном процессе маршрутизации только IP-адрес получателя определяет то, каким образом будет передан пакет. При необходимости изменения стандартного процесса маршрутизации используется маршрутизация на основе определённых политик (Policy-Based Routing – PBR). Выборка нужных пакетов осуществляется посредством использования гибких фильтров трафика.

Политики маршрутизации трафика — это механизм, позволяющий изменять маршрут следования пакетов, соответствующих критериям определённого фильтра, согласно указанным таблицам маршрутизации. Например можно задать конкретный шлюз или интерфейс, через который должна происходить доставка пакетов. При этом маршрутизация трафика согласно определённой политике производится только в случае её применения к конкретному интерфейсу.

В настройках Numa Edge политики маршрутизации трафика сгруппированы узлом **policy route** который служит контейнером для операторов политики. Действующими операторами политики определяются правила обработки пакетов.

Политики маршрутизации трафика применяются первыми после получения данных, перед применением правил МЭ, политик модификации трафика и политик QoS.

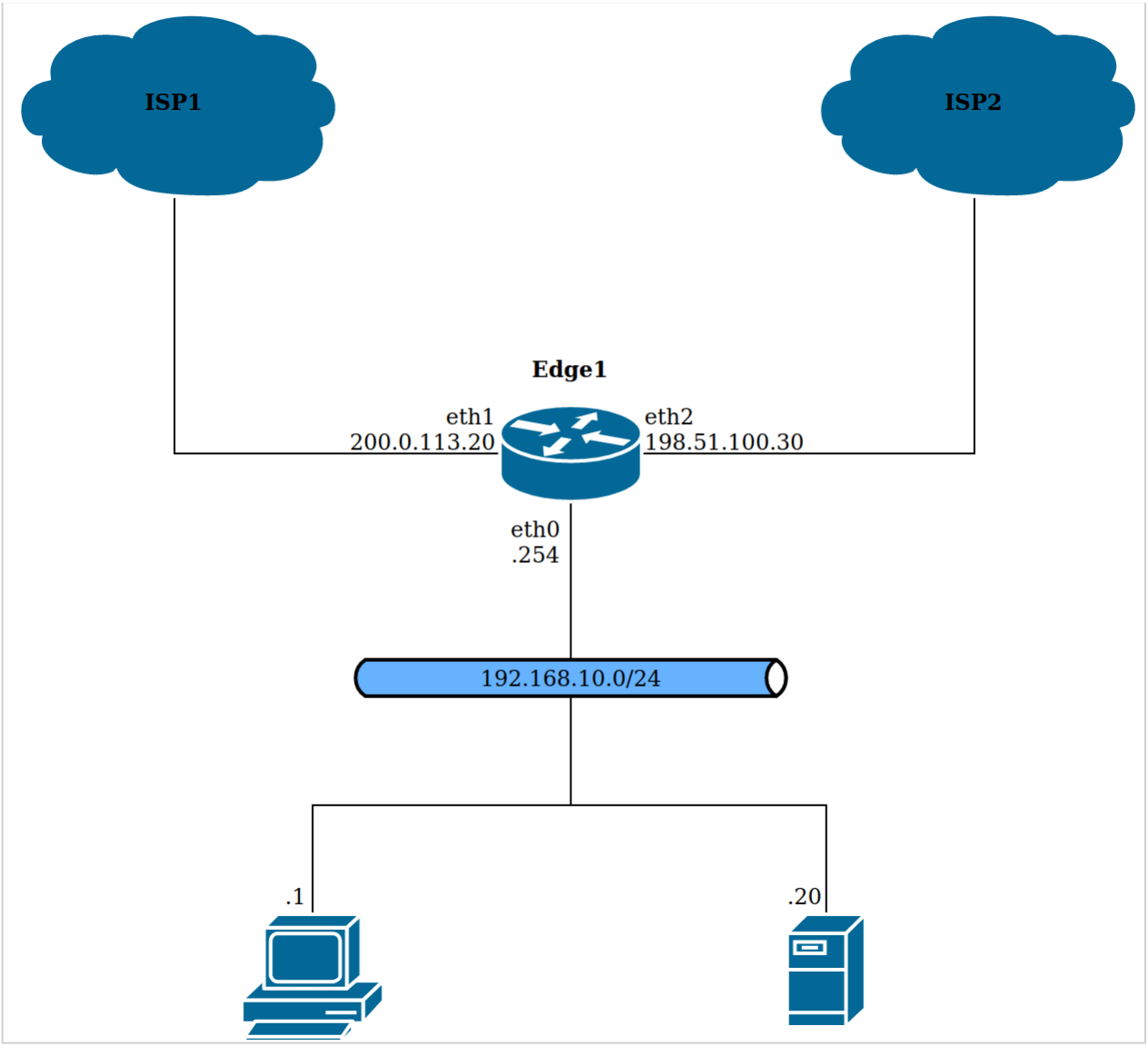


Рисунок 75 – Схема стенда

Политика маршрутизации трафика представляет собой именованный упорядоченный набор правил маршрутизации. Каждое правило содержит критерий соответствия на основе определённого фильтра. Так как правила политики упорядочены, маршрутизация производится в порядке нумерации правил. То есть при наличии нескольких правил с одним и тем же фильтром в качестве критерия соответствия в рамках одной политики, маршрутизация будет производиться согласно правилу с наименьшим номером.

32.2 Примеры настройки политик маршрутизации трафика

В данном разделе приведены примеры настройки для политик маршрутизации трафика. Здесь рассматриваются следующие вопросы:

- Пример настройки и применения политики маршрутизации трафика при наличии двух каналов связи с различающимися характеристиками.
- Пример настройки и применения политики маршрутизации трафика при наличии двух каналов связи для обеспечения одновременного использования их пропускной способности.

32.2.1 Пример настройки и применения политики маршрутизации трафика при наличии двух каналов связи с различающимися характеристиками

Numa Edge является шлюзом в локальной сети с двумя каналами связи для доступа к сети Интернет. Провайдер ISP1 имеет канал с большой пропускной способностью, но с большими задержками подключается и доступен через интерфейс Ethernet **eth1** с IP-адресом 200.0.113.20. Провайдер ISP2 с малой пропускной способностью, но с малыми задержками, подключается к интерфейсу **eth2** с IP-адресом 198.51.100.30. IP-адрес

шлюза ISP1 — 200.0.113.55, шлюза ISP2 — 198.51.100.55. Шлюз локальной сети располагается на интерфейсе Ethernet **eth0**. Пакеты трафика чувствительного к задержкам определяются по установленному значению поля DSCP (lowdelay) и направляется на интерфейс **eth2**, весь остальной трафик направляется на интерфейс **eth1**.

Для решения этого примера необходимо выполнить следующие действия:

- Произвести настройка интерфейсов eth1 и eth2;
- Создать фильтр трафика с именем "Low_latency" с правилом определения пакетов со значением lowdelay поля DSC;
- Создать таблицы маршрутизации ISP1_table с указанием статического маршрута 0.0.0.0/0 – 200.0.113.55 и ISP2_table с указанием статического маршрута 0.0.0.0/0 – 198.51.100.55;
- Создать политику маршрутизации трафика ISP1_ISP2 с указанием фильтра Low_latancy и таблиц маршрутизации ISP1_table и ISP2_table;
- Применить политика маршрутизации ISP1_ISP2 к интерфейсу **eth0**.

Для выполнения данной настройки необходимо выполнить следующую последовательность команд в режиме настройки:

Пример 308 - Пример настройки и применения политики маршрутизации трафика при наличии двух каналов связи с различающимися характеристиками

Действие	**Команда**
Указание IP-адреса 200.0.113.20/24 в качестве IP-адреса для интерфейса Ethernet eth1.	`[edit]` `admin@edge# set interfaces ethernet eth1 address 200.0.113.20/24`
Указание IP-адреса 198.51.100.30/24 в качестве IP-адреса для интерфейса Ethernet eth2.	`[edit]` `admin@edge# set interfaces ethernet eth2 address 198.51.100.30/24`
Создание фильтра трафика с именем Low_latancy. Указание текстового описания.	`[edit]` `admin@edge# set filter Low_latancy description "filter for low latancy"`
Создание правила на определение пакетов по полю DSCP.	`[edit]` `admin@edge# set filter Low_latancy rule 10 dscp 4`
Фиксация изменений.	`[edit]` `admin@edge# commit`

Вывод настроек фильтра трафика Low_latancy.	`[edit]`
	`admin@edge# show filter Low_latancy`
	`description "filter for low latancy"`
	`rule 10 {`
	`dscp 4`
	`}`

Определение таблицы маршрутизации с именем ISP1_table.	`[edit]` `admin@edge# set protocols static table ISP1_table`
Указание статического маршрута 0.0.0.0/0 — 200.0.113.55 в таблице маршрутизации ISP1_table.	`[edit]` `admin@edge# set protocols static table ISP1_table route 0.0.0.0/0 next-hop 200.0.113.55`
Фиксация изменений.	`[edit]` `admin@edge# commit`

Вывод настроек таблицы маршрутизации ISP1_table.	`[edit]`
	`admin@edge# show protocols static table ISP1_table`
	`route 0.0.0.0/0 {`
	`next-hop 200.0.113.55 {`
	`}`
	`}`

Определение таблицы маршрутизации с именем ISP2_table.	`[edit]` `admin@edge# set protocols static table`

Действие	**Команда**
	`ISP2_table`
Указание статического маршрута 0.0.0.0/0 — 198.51.100.55 в таблице маршрутизации ISP2_table.	`[edit]` `admin@edge# set protocols static table ISP2_table route 0.0.0.0/0 next-hop 198.51.100.55`
Фиксация изменений.	`[edit]` `admin@edge# commit`

Вывод настроек таблицы маршрутизации ISP2_table.	`[edit]`
	`admin@edge# show protocols static table ISP2_table`
	`route 0.0.0.0/0 {`
	`next-hop 198.51.100.55 {`
	`}`
	`}`

Определение политики маршрутизации трафика.	`[edit]` `admin@edge# set policy route ISP1_ISP2`
Указание определённого фильтра трафика для правила данной политики маршрутизации трафика.	`[edit]` `admin@edge# set policy route ISP1_ISP2 rule 10 match filter Low_latancy`
Указание определённой таблицы маршрутизации для правила данной политики маршрутизации трафика.	`[edit]` `admin@edge# set policy route ISP1_ISP2 rule 10 table ISP2_table`
Указание определённой таблицы маршрутизации для правила данной политики маршрутизации трафика.	`[edit]` `admin@edge# set policy route ISP1_ISP2 rule 20 table ISP1_table`
Фиксация изменений.	`[edit]` `admin@edge# commit`

Вывод настроек политики маршрутизации трафика E1-satellite.	`[edit]`
	`admin@edge# show policy route ISP1_ISP2`
	`rule 10 {`
	`match {`
	`filter Low_latancy`
	`}`
	`table ISP2_table {`
	`}`
	`}`
	`rule 20 {`
	`table ISP1_table {`
	`}`
	`}`

Указание применения определённой политики маршрутизации трафика для для входящего трафика на интерфейсе Ethernet eth2.	`[edit]` `admin@edge# set interfaces ethernet eth0 policy in route ISP1_ISP2`
Фиксация изменений.	`[edit]` `admin@edge# commit`

Вывод настроек интерфейса Ethernet eth0.	`[edit]`
	`admin@edge# show interfaces ethernet eth0`
	`policy {`
	`in {`
	`route ISP1_ISP2`
	`}`
	`}`

32.2.2 Пример настройки и применения политики маршрутизации трафика при наличии двух каналов связи для обеспечения одновременного использования их пропускной способности

Numa Edge является шлюзом в локальной сети с двумя каналами связи для доступа к сети Интернет, как показано на рисунке ниже. Шлюз локальной сети располагается на интерфейсе Ethernet **eth0** IP-адресом 192.168.10.254. Локальная сеть обслуживает клиентов с IP-адресами в диапазоне 192.168.10.1 — 192.168.10.200. Первый провайдер подключен к интерфейсу Ethernet **eth1** с IP-адресом 192.168.12.1/24, второй — к интерфейсу Ethernet **eth2** с IP-адресом 192.168.13.1/24. IP-адрес шлюза первого провайдера — 192.168.12.2, второго — 192.168.13.3. Оба провайдера маршрутизируют только пакеты с адресами источника из своих сетей. Данное ограничение введено для предупреждения возможности атаки с подменой адреса отправителя (спуфинг). На Numa Edge настроено преобразование сетевого адреса получателя (DNAT) пакетов, полученных на порт номер 80. Также осуществляется преобразование сетевого адреса отправителя пакетов (SNAT), при отправке пакетов из внутренней сети.

Необходимо создать условия для одновременного использования пропускной способности обоих каналов подключения к интернету, соблюдая требование провайдеров относительно обеспечения симметричной маршрутизации входящих и исходящих пакетов. Кроме того, симметричная маршрутизация также должна обеспечиваться для внутреннего трафика Numa Edge.

Для решения этого примера необходимо выполнить следующие действия:

- Произвести настройку интерфейсов Ethernet **eth1** и **eth2** с присвоением IP-адресов 192.168.12.10/24 и 192.168.13.10/24.
- Произвести настройку службы NAT таким образом, чтобы все узлы подсети 192.168.10.0/24 использовали внешние IP-адреса интерфейсов Ethernet **eth1** и **eth2**, при этом доступ к данной подсети извне осуществлялся через порт номер 80.
- Создать фильтры трафика ISP1_filter и ISP2_filter с правилом определения пакетов с IP-адресов 192.168.12.0/24 и 192.168.13.0/24 соответственно.
- Создать таблицы маршрутизации ISP1_table с настроенным статическим маршрутом 0.0.0.0/0 — 192.168.12.2 и ISP2_table с настроенным статическим маршрутом 0.0.0.0/0 — 192.168.13.3.
- Определить политику маршрутизации трафика ISP1_ISP2 с указанием фильтров ISP1_filter и ISP2_filter, а также таблиц маршрутизации ISP1_table и ISP2_table.
- Применить политику маршрутизации ISP1_ISP2 к локальному трафику и к интерфейсу Ethernet **eth0**.

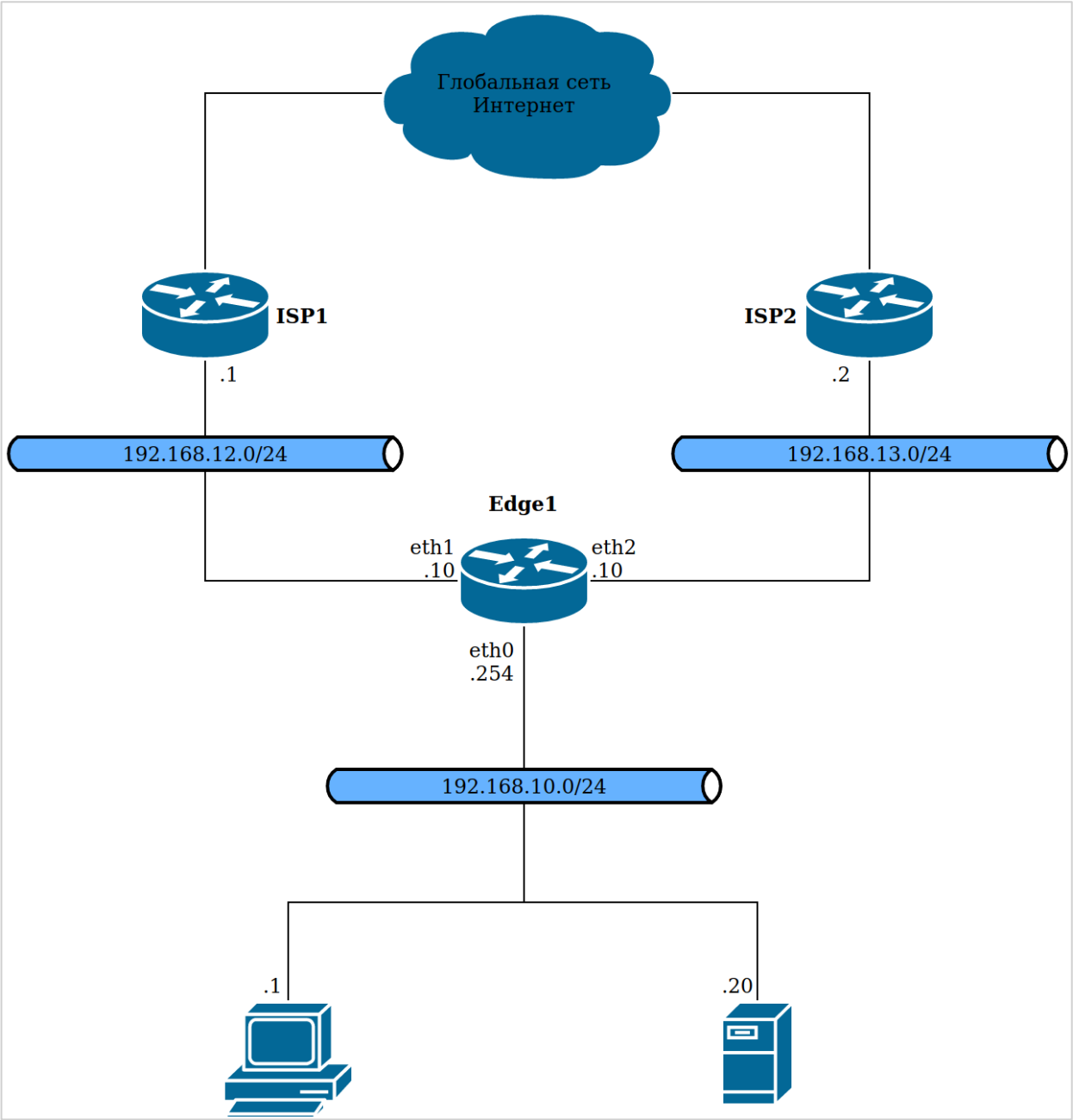


Рисунок 76- Пример использования Numa Edge в качестве шлюза локальной сети при наличии подключения к двум провайдерам интернета.

Для выполнения данной настройки необходимо выполнить следующую последовательность команд в режиме настройки:

Пример 309 - Пример настройки и применения политики маршрутизации трафика при наличии двух каналов связи для обеспечения одновременного использования их пропускной способности

Действие	**Команда**
Указание IP-адреса 192.168.10.254/24 для интерфейса Ethernet eth0.	`[edit]` `admin@edge# set interfaces ethernet eth0 address 192.168.10.254/24`
Указание IP-адреса 192.168.12.10/24 для интерфейса Ethernet eth1.	`[edit]` `admin@edge# set interfaces ethernet eth1 address 192.168.12.10/24`
Указание IP-адреса 192.168.13.10/24 для интерфейса Ethernet eth2.	`[edit]` `admin@edge# set interfaces ethernet eth2 address 192.168.13.10/24`

Действие	**Команда**
Создание правила преобразования сетевого адреса отправителя (SNAT).	[edit] admin@edge# set service nat ipv4 rule 10 type source
Применение данного правила к пакетам, которые были отправлены любым узлом сети 192.168.10.0/24.	[edit] admin@edge# set service nat ipv4 rule 10 source address 192.168.10.0/24
Отправка трафика через интерфейс eth1. Адрес 192.168.12.10 используется в качестве адреса отправителя для исходящих сетевых пакетов. Следует учесть, что внешний адрес должен быть одним из адресов, определенных на выходном интерфейсе.	[edit] admin@edge# set service nat ipv4 rule 10 outbound-interface eth1 [edit] admin@edge# set service nat ipv4 rule 10 outside-address address 192.168.12.10
Создание правила преобразования сетевого адреса отправителя (SNAT).	[edit] admin@edge# set service nat ipv4 rule 20 type source
Применение данного правила к пакетам, которые были отправлены любым узлом сети 192.168.10.0/24.	[edit] admin@edge# set service nat ipv4 rule 20 source address 192.168.10.0/24
Отправка трафика через интерфейс eth2. Адрес 192.168.13.10 используется в качестве адреса отправителя для исходящих сетевых пакетов. Следует учесть, что внешний адрес должен быть одним из адресов, определенных на выходном интерфейсе.	[edit] admin@edge# set service nat ipv4 rule 20 outbound-interface eth2 [edit] admin@edge# set service nat ipv4 rule 20 outside-address address 192.168.13.10
Создание преобразования сетевого адреса получателя (DNAT).	[edit] admin@edge# set service nat ipv4 rule 30 type destination
Применение данного правила к пакетам протокола tcp.	[edit] admin@edge# set service nat ipv4 rule 30 protocol tcp
Применение данного правила на интерфейсе eth1 для порта номер 80	[edit] admin@edge# set service nat ipv4 rule 30 inbound-interface eth1 [edit] admin@edge# set service nat ipv4 rule 30 destination port 80
Пересылка трафика на адрес 192.168.10.20.	[edit] admin@edge# set service nat ipv4 rule 30 inside-address address 192.168.10.20
Создание преобразования сетевого адреса получателя (DNAT).	[edit] admin@edge# set service nat ipv4 rule 40 type destination
Применение данного правила к пакетам протокола tcp.	[edit] admin@edge# set service nat ipv4 rule 40 protocol tcp
Применение данного правила на интерфейсе eth2 для порта номер 80	[edit] admin@edge# set service nat ipv4 rule 40 inbound-interface eth2 [edit] admin@edge# set service nat ipv4 rule 40 destination port 80
Пересылка трафика на адрес 192.168.10.20.	[edit] admin@edge# set service nat ipv4 rule 40 inside-address address 192.168.10.20
Фиксация изменения.	[edit] admin@edge# commit
Вывод настройки NAT.	admin@edge# show service nat ipv4 rule

Действие	Команда

	10 {
	outbound-interface eth1
	outside-address {
	address 192.168.12.10
	}
	source {
	address 192.168.10.0/24
	}
	type source
	}
	20 {
	outbound-interface eth2
	outside-address {
	address 192.168.13.10
	}
	source {
	address 192.168.10.0/24
	}
	type source
	}
	30 {
	destination {
	port 80
	}
	inbound-interface eth1
	inside-address {
	address 192.168.10.20
	}
	protocol tcp
	type destination
	}
	40 {
	destination {
	port 80
	}
	inbound-interface eth2
	inside-address {
	address 192.168.10.20
	}
	protocol tcp
	type destination
	}

Создание фильтра трафика первого провайдера (ISP1_filter). Указание краткого текстового описания.	[edit] admin@edge# set filter ISP1_filter description "ISP1 traffic filter"
Создание правила на трафика первого провайдера.	[edit] admin@edge# set filter ISP1_filter rule 10 source address 192.168.12.0/24
Фиксация изменений.	[edit] admin@edge# commit

Вывод настроек фильтра.	[edit]
	admin@edge# show filter ISP1_filter
	description "ISP1 traffic filter"
	rule 10 {
	source {
	address 192.168.12.0/24
	}
	}

Создание фильтра трафика второго провайдера (ISP2_filter). Указание краткого текстового	[edit] admin@edge# set filter ISP2_filter description "ISP2 traffic filter"

Действие	**Команда**
описания.	
Создание правила на трафика второго провайдера.	`[edit]` `admin@edge# set filter ISP2_filter rule 10 source address 192.168.13.0/24`
Фиксация изменений.	`[edit]` `admin@edge# commit`

Вывод настроек фильтра.	`[edit]`
	`admin@edge# show filter ISP2_filter`
	`description "ISP2 traffic filter"`
	`rule 10 {`
	`source {`
	`address 192.168.13.0/24`
	`}`
	`}`

Создание таблицы маршрутизации ISP1_table. Указание статического маршрута 0.0.0.0/0 — 192.168.12.10.	`[edit]` `admin@edge# set protocols static table ISP1_table route 0.0.0.0/0 next-hop 192.168.12.2`
Создание таблицы маршрутизации ISP2_table. Указание статического маршрута 0.0.0.0/0 — 192.168.13.10.	`[edit]` `admin@edge# set protocols static table ISP2_table route 0.0.0.0/0 next-hop 192.168.13.3`
Фиксация изменений.	`[edit]` `admin@edge# commit`

Вывод настроек созданных таблиц маршрутизации.	`[edit]`
	`admin@edge# show protocols static table`
	`ISP1_table {`
	`route 0.0.0.0/0 {`
	`next-hop 192.168.12.2 {`
	`}`
	`}`
	`}`
	`ISP2_table {`
	`route 0.0.0.0/0 {`
	`next-hop 192.168.13.3 {`
	`}`
	`}`
	`}`

Создание политики маршрутизации трафика ISP1_ISP2. Указание определённого фильтра трафика для правила данной политики маршрутизации трафика.	`[edit]` `admin@edge# set policy route ISP1_ISP2 rule 10 match filter ISP1_filter`
Указание определённой таблицы маршрутизации для правила данной политики маршрутизации трафика.	`[edit]` `admin@edge# set policy route ISP1_ISP2 rule 10 table ISP1_table`
Указание определённого фильтра трафика для правила данной политики маршрутизации трафика.	`[edit]` `admin@edge# set policy route ISP1_ISP2 rule 20 match filter ISP2_filter`
Указание определённой таблицы маршрутизации для правила данной политики маршрутизации трафика.	`[edit]` `admin@edge# set policy route ISP1_ISP2 rule 20 table ISP2_table`

Создание правила с одновременным указанием таблиц ISP1_table и ISP2_table.	`[edit]`
	`admin@edge# set policy route ISP1_ISP2 rule 30 table ISP1_table`
	`[edit]`
	`admin@edge# set policy route ISP1_ISP2 rule 30 table ISP2_table`

Фиксация изменений.	`[edit]`

Действие	Команда
	admin@edge# commit

Вывод настроек политики маршрутизации трафика 2xISP.	admin@edge#show policy route ISP1_ISP2
	rule 10 {
	match {
	filter ISP1_filter
	}
	table ISP1_table {
	}
	}
	rule 20 {
	match {
	filter ISP2_filter
	}
	table ISP2_table {
	}
	}
	rule 30 {
	table ISP1_table {
	}
	table ISP2_table {
	}
	}

Указание применения определённой политики маршрутизации к локальному трафику	[edit] admin@edge# set system policy route ISP1_ISP2
Фиксация изменений.	[edit] admin@edge# commit
Вывод настройки политики маршрутизации для локального трафика.	[edit] admin@edge# show system policy route ISP1_ISP2
Указание применения определённой политики маршрутизации трафика для для входящего трафика на интерфейсе Ethernet eth0.	[edit] admin@edge# set interfaces ethernet eth0 policy in route ISP1_ISP2
Фиксация изменений.	[edit] admin@edge# commit

Вывод настроек интерфейса Ethernet eth0.	[edit]
	admin@edge# show interfaces ethernet eth0
	address 192.168.10.254/24
	policy {
	in {
	route ISP1_ISP2
	}
	}

32.3 Команды политик маршрутизации трафика

В данном разделе описаны команды политик маршрутизации системы Numa Edge.

Таблица 265 - Команды политик маршрутизации трафика.

Режим настройки	
Применение политик маршрутизации трафика к интерфейсам	
interfaces <интерфейс> policy in route <имя_политики>	Указание применения политики маршрутизации трафика для заданного интерфейса.
interfaces <интерфейс> policy in route-ipv6 <имя_политики>	Указание применения политики маршрутизации трафика IPv6 для заданного интерфейса.
Применение таблицы маршрутизации трафика к локальному трафику	
system policy route <имя_политики>	Применение политики маршрутизации трафика к локальному трафику.

Команды политик маршрутизации трафика	
policy route <имя_политики>	Определение имени политики маршрутизации трафика.
policy route <имя_политики> description <описание>	Создание текстового описания для указанной политики маршрутизации трафика.
policy route <имя_политики> flow-balancing <состояние>	Включение или отключение маршрутизации потоков трафика для данной политики маршрутизации трафика.
policy route <имя_политики> rule <номер_правила> description <описание>	Задание текстового описания для правила в указанной политики маршрутизации трафика.
policy route <имя_политики> rule <номер_правила>	Создание правила для политики маршрутизации трафика.
policy route <имя_политики> rule <номер_правила> log <состояние>	Включение/выключение регистрации событий маршрутизации трафика для указанного правила указанной политики.
policy route <имя_политики> rule <номер_правила> match filter <имя_фильтра>	Указание применения определённого фильтра трафика в правиле политики маршрутизации трафика.
policy route <имя_политики> rule <номер_правила> table <имя_таблицы>	Указание применения определённой таблицы маршрутизации в правиле политики маршрутизации трафика.
policy route <имя_политики> rule <номер_правила> table <имя_таблицы> failover-table	Использовать определённую таблицу маршрутизации в качестве резервной, если другие таблицы недоступны.
policy route <имя_политики> rule <номер_правила> table <имя_таблицы> weight <вес_таблицы>	Указание веса определённой таблицы маршрутизации.
policy route-ipv6 <имя_политики>	Определение политики маршрутизации трафика IPv6.
policy route-ipv6 <имя_политики> description <описание>	Создание текстового описания для указанной политики маршрутизации трафика IPv6.
policy route-ipv6 <имя_политики> flow-balancing <состояние>	Включение или отключение балансировки соединений для данной политики маршрутизации трафика IPv6.
policy route-ipv6 <имя_политики> rule <номер_правила>	Создание правила для политики маршрутизации трафика IPv6.
policy route-ipv6 <имя_политики> rule <номер_правила> description <описание>	Задание текстового описания для правила в указанной политики маршрутизации трафика IPv6.
policy route-ipv6 <имя_политики> rule <номер_правила> log <состояние>	Включение или отключение протоколирования правила данной политики маршрутизации трафика IPv6.
policy route-ipv6 <имя_политики> rule <номер_правила> match filter-ipv6 <имя_фильтра>	Указание применения определённого фильтра трафика IPv6 для данной политики маршрутизации трафика IPv6.
policy route-ipv6 <имя_политики> rule <номер_правила> table <имя_таблицы>	Указание применения определённой таблицы маршрутизации для данной политики маршрутизации трафика IPv6.
policy route-ipv6 <имя_политики> rule <номер_правила> table <имя_таблицы> failover-table	Использовать определённую таблицу маршрутизации только если другие таблицы недоступны.
policy route-ipv6 <имя_политики> rule <номер_правила> table <имя_таблицы> weight <вес>	Указание веса определённой таблицы маршрутизации.
Эксплуатационные команды	
policy clear route <имя_политики>	Очистка статистики указанной политики маршрутизации.
policy clear route <имя_политики> rule <номер_правила>	Очистка статистики правила политики маршрутизации.
policy clear route <имя_политики> rule <номер_правила> filter	Очистка статистики по фильтру, связанному с указанным правилом политики маршрутизации.
policy clear route <имя_политики> rule <номер_правила> filter rule <номер_правила>	Очистка статистики для указанного правила фильтра, связанного с указанным правилом политики маршрутизации.
policy show route <имя_политики>	Вывод сведений и статистики указанной политики маршрутизации.

policy show route <имя_политики> rule <номер_правила>	Вывод сведений и статистики указанного правила политики маршрутизации.
policy show route <имя_политики> rule <номер_правила> filter	Вывод сведений о фильтре, связанном с указанным правилом.
policy show route <имя_политики> rule <номер_правила> filter rule <номер_правила>	Вывод подробных сведений о конфигурации и статистики по указанному правилу фильтра, связанного с указанным правилом политики маршрутизации.

32.3.1 interfaces <интерфейс> policy in route <имя_политики>

Указание применения политики маршрутизации трафика для заданного интерфейса.

Синтаксис

```
set interfaces <интерфейс> policy in route <имя_политики>

delete interfaces <интерфейс> policy in route

show interfaces <интерфейс> policy in route
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
   policy {
      in {
         route имя_политики
      }
   }
}
```

Параметры

интерфейс

Интерфейс, к которому применяется политика маршрутизации трафика. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже в разделе Указания по использованию.

имя_политики

Имя политики маршрутизации трафика, применяемой к данному интерфейсу.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для применения политики маршрутизации трафика к интерфейсу.

В приведенной ниже таблице показаны типы поддерживаемых интерфейсов и синтаксис.

Таблица 266 – Типы интерфейсов

Тип интерфейса	Синтаксис
Агрегирование каналов	bonding bondx
Виртуальный интерфейс агрегированных каналов	bonding bondx vif идентификатор_vlan
Сетевой мост	bridge brx
Ethernet	ethernet ethx
Ethernet PPPoE	ethernet ethx pppoe номер
Виртуальный интерфейс Ethernet	ethernet ethx vif идентификатор_vlan
Ethernet Vif PPPoE	ethernet ethx vif идентификатор_vlan pppoe номер
Интерфейс заглушки	loopback lo

Многоканальная связь	multilink mlx
OpenVPN	openvpn vtunx
Псевдо-Ethernet	pseudo-ethernet pethx
Последовательный интерфейс	serial srx vif идентификатор_vlan
Туннель	tunnel tunx

Форма **set** этой команды используется для применения политики маршрутизации трафика к интерфейсу.

Форма **delete** этой команды используется для удаления политики маршрутизации трафика с интерфейса.

Форма **show** этой команды используется для отображения настройки политики маршрутизации трафика на интерфейсе.

32.3.2 interfaces <интерфейс> policy in route-ipv6 <имя_политики>

Указание применения политики маршрутизации трафика IPv6 для заданного интерфейса.

Синтаксис

```
set interfaces <интерфейс> policy in route-ipv6 <имя_политики>
delete interfaces <интерфейс> policy in route-ipv6
show interfaces <интерфейс> policy in route-ipv6
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
   policy {
      in {
         route-ipv6 имя_политики
      }
   }
}
```

Параметры

интерфейс

Интерфейс, к которому применяется политика маршрутизации трафика IPv6. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже в разделе Указания по использованию.

имя_политики

Имя политики маршрутизации трафика IPv6, применяемой к данному интерфейсу.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для применения политики маршрутизации трафикаIPv6 к интерфейсу.

В приведенной ниже таблице показаны типы поддерживаемых интерфейсов и синтаксис.

Таблица 267 – Типы интерфейсов

Тип интерфейса	**Синтаксис**
Агрегирование каналов	bonding bondx
Виртуальный интерфейс агрегированных каналов	bonding bondx vif идентификатор_vlan
Сетевой мост	bridge brx
Ethernet	ethernet ethx
Ethernet PPPoE	ethernet ethx pppoe номер

Виртуальный интерфейс Ethernet	ethernet ethx vif идентификатор_vlan
Ethernet Vif PPPoE	ethernet ethx vif идентификатор_vlan pppoe номер
Интерфейс заглушки	loopback lo
Многоканальная связь	multilink mlx
OpenVPN	openvpn vtunx
Псевдо-Ethernet	pseudo-ethernet pethx
Последовательный интерфейс	serial srx vif идентификатор_vlan
Туннель	tunnel tunx

Форма **set** этой команды используется для применения политики маршрутизации трафика IPv6 к интерфейсу.

Форма **delete** этой команды используется для удаления политики маршрутизации трафика IPv6 с интерфейса.

Форма **show** этой команды используется для отображения настройки политики маршрутизации трафика IPv6 на интерфейсе.

32.3.3 system policy route <имя_политики>

Применение политики маршрутизации трафика к локальному трафику.

Синтаксис

```
set system policy route <имя_политики>
delete system policy route
show  system policy route
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
system {
   policy {
      route имя_политики
   }
}
```

Параметры

имя_политики

Имя политики маршрутизации трафика, применяемой к локальному трафику.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для применения политики маршрутизации трафика к локальному трафику.

ПРИМЕЧАНИЕ в системе Numa Edge маршрутизация локального трафика, согласно указанной политике, будет производится только при условии наличия локального маршрута в основной таблице маршрутизации. Если локальный маршрут не прописан в основной таблице маршрутизации, то система Numa Edge будет выдавать ошибку «Network is unreachable», даже при условии наличия маршрута в политике маршрутизации. При этом, если локальный маршрут прописан в основной таблице маршрутизации и одновременно применяется политика маршрутизации трафика, то маршрутизация будет производиться согласно политике маршрутизации трафика.

Форма **set** этой команды используется для применения политики маршрутизации трафика к локальному трафику.

Форма **delete** этой команды используется для отмены использования политики маршрутизации трафика для локального трафика.

Форма **show** этой команды используется для отображения настройки политики маршрутизации трафика для локального трафика.

32.3.4 policy route <имя_политики>

Определение имени политики маршрутизации трафика.

Синтаксис

```
set policy route <имя_политики>
delete policy route <имя_политики>
show policy route <имя_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route имя_политики
}
```

Параметры

имя_политики

Имя политики маршрутизации трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет определить имя политики маршрутизации трафика.

Форма **set** данной команды используется для определения имени политики.

Форма **delete** используется для удаления политики.

Форма **show** используется для отображения настроек политики маршрутизации трафика.

32.3.5 policy route <имя_политики> description <описание>

Создание текстового описания для указанной политики маршрутизации трафика.

Синтаксис

```
set policy route <имя_политики> description <описание>
delete policy route <имя_политики> description
show policy route <имя_политики> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route имя_политики {
        description описание
    }
}
```

Параметры

имя_политики

Имя политики маршрутизации трафика.

описание

Текстовое описание политики. В том случае если описание содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для задания текстового описания для указанной политики.

Форма **delete** используется для удаления описания.

Форма **show** используется для отображения описания.

32.3.6 policy route <имя_политики> flow-balancing <состояние>

Включение или отключение маршрутизации потоков трафика для данной политики маршрутизации трафика.

Синтаксис

```
set policy route <имя_политики> flow-balancing <состояние>
delete policy route <имя_политики> flow-balancing
show policy route <имя_политики> flow-balancing
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route имя_политики {
      flow-balancing состояние
   }
}
```

Параметры

имя_политики

Имя политики маршрутизации трафика.

состояние

Включение или отключение маршрутизации потоков трафика. Поддерживаются следующие значения:

enable: Включить маршрутизацию потоков трафика.

disable: Выключить маршрутизацию отдельных пакетов.

Значение по умолчанию

enable. Включена маршрутизация потока трафика для данной политики маршрутизации трафика.

Указания по использованию

Данная команда используется для включения или отключения маршрутизации потоков трафика для данной политики модификации трафика. При значении enable все пакеты, относящиеся к единому потоку будут направлены по одному и тому же маршруту. При значении disable пакеты, относящиеся к единому потоку могут быть направлены по разным маршрутам.

Форма **set** данной команды используется для включения или отключения маршрутизации потока трафика.

Форма **delete** используется для установки значения по умолчанию.

Форма **show** используется для отображения текущего значения.

32.3.7 policy route <имя_политики> rule <номер_правила>

Создание правила для политики маршрутизации трафика.

Синтаксис

```
set policy route <имя_политики> rule <номер_правила>
delete policy route <имя_политики> rule <номер_правила>
show policy route <имя_политики> rule <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route имя_политики {
        rule номер_правила {
        }
    }
}
```

Параметры

имя_политики

Множественный узел. Текстовый идентификатор политики маршрутизации трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Значение должно лежать в диапазоне 1-65535.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания правила для политики маршрутизации трафика.

Форма **delete** этой команды используется для удаления правила для политики маршрутизации трафика.

Форма **show** этой команды используется для отображения параметров настройки правила политики маршрутизации трафика.

32.3.8 policy route <имя_политики> rule <номер_правила> description <описание>

Задание текстового описания для правила в указанной политики маршрутизации трафика.

Синтаксис

```
set policy route <имя_политики> rule <номер_правила> description <описание>
delete policy route <имя_политики> rule <номер_правила> description
show policy route <имя_политики> rule <номер_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route имя_политики {
        rule номер_правила {
            description описание
        }
```

```
    }
}
```

Параметры

имя_политики

Имя политики маршрутизации трафика.

описание

Текстовое описание политики. В том случае если описание содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для задания текстового описания для указанной политики.

Форма **delete** используется для удаления описания.

Форма **show** используется для отображения описания.

32.3.9 policy route <имя_политики> rule <номер_правила> log <состояние>

Включение/выключение регистрации событий маршрутизации трафика для указанного правила указанной политики.

Синтаксис

```
set policy route <имя_политики> rule <номер_правила> log <состояние>
delete policy route <имя_политики> rule <номер_правила> log
show policy route <имя_политики> rule <номер_правила> log
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route имя_политики {
        rule номер_правила {
            log состояние
        }
    }
}
```

Параметры

имя_политики

Имя определённой политики маршрутизации трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

состояние

Включение или отключение протоколирование правил политики. Поддерживаются следующие значения:

enable: Включить протоколирование правил политики.

disable: Выключить протоколирование правил политики

Значение по умолчанию

Отсутствует.

Указания по использованию

В том случае, если задействовано журналирование для правила политики, в системный лог (журнал) будут выводиться сообщения для всех пакетов, подпадающих под правило. Для каждого сообщения формируется префикс в квадратных скобках ([r-<имя>-<номер правила>-<имя таблицы маршрутизации>]). Имя политики (<имя>) и/или таблицы (<имя таблицы маршрутизации>) может быть записано в журнале не полностью в связи с системным ограничением общей длины префикса в 29 символов.

Форма **set** этой команды используется для задания настройки регистрации событий маршрутизации трафика для указанного правила указанной политики.

Форма **delete** этой команды используется для удаления настройки регистрации событий маршрутизации.

Форма **show** этой команды используется для отображения настройки регистрации событий маршрутизации.

32.3.10 policy route <имя_политики> rule <номер_правила> match filter <имя_фильтра>

Указание применения определённого фильтра трафика в правиле политики маршрутизации трафика.

Синтаксис

```
set policy route <имя_политики> rule <номер_правила> match filter <имя_фильтра>

delete policy route <имя_политики> rule <номер_правила> match

show policy route <имя_политики> rule <номер_правила> match
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route имя_политики {
        rule номер_правила {
            match {
                filter имя_фильтра
            }
        }
    }
}
```

Параметры

имя_политики

Имя политики маршрутизации трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

имя_фильтра

Имя применяемого фильтра трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания применения определённого фильтра трафика в правиле политики модификации трафика.

Форма **set** данной команды используется для указания применения определённого фильтра.

Форма **delete** используется для отмены применения определённого фильтра.

Форма **show** используется для отображения текущего значения.

32.3.11 policy route <имя_политики> rule <номер_правила> table <имя_таблицы>

Указание применения определённой таблицы маршрутизации в правиле политики маршрутизации трафика.

Синтаксис

```
set policy route <имя_политики> rule <номер_правила> table <имя_таблицы>
delete policy route <имя_политики> rule <номер_правила> table <имя_таблицы>
show policy route <имя_политики> rule <номер_правила> table <имя_таблицы>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route имя_политики {
      rule номер_правила {
         table имя_таблицы
      }
   }
}
```

Параметры

имя_политики

Имя политики маршрутизации трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

имя_таблицы

Имя таблицы маршрутизации трафика. Возможно указание нескольких таблиц маршрутизации в рамках одного правила.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать применение определённой таблицы маршрутизации в правиле политики маршрутизации трафика. При указании нескольких таблиц маршрутизации вероятность выбора одной из таблиц определяется значением её веса. Значение веса указанной таблицы маршрутизации задаётся командой **policy route <имя_политики> rule <номер_правила> table <имя_таблицы> weight <вес_таблицы>**.

Форма **set** данной команды используется для указания применения определённой таблицы маршрутизации трафика.

Форма **delete** используется для удаления определённой таблицы маршрутизации трафика из правила политики маршрутизации.

Форма **show** используется для отображения текущей используемой таблиц маршрутизации трафика для данной политики маршрутизации.

32.3.12 policy route <имя_политики> rule <номер_правила> table <имя_таблицы> failover-table

Использовать определённую таблицу маршрутизации в качестве резервной, если другие таблицы недоступны.

Синтаксис

```
set policy route <имя_политики> rule <номер_правила> table <имя_таблицы> failover-table
```

```
delete policy route <имя_политики> rule <номер_правила> table <имя_таблицы> failover-table
```

```
show policy route <имя_политики> rule <номер_правила> table <имя_таблицы> failover-table
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route имя_политики {
        rule номер_правила {
            table имя_таблицы {
                failover-table
            }
        }
    }
}
```

Параметры

имя_политики

Имя политики маршрутизации трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65535. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

имя_таблицы

Имя таблицы маршрутизации трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет определить таблицу маршрутизации как резервную. То есть она будет использоваться только в случае определения неработоспособности остальных таблиц сервисом балансировки нагрузки.

Если в системе присутствуют две или более резервные таблицы маршрутизации, то приоритет конкретной таблицы в рамках политики маршрутизации определяется значением веса таблицы. В случае присутствия в

системе двух и более резервных таблиц маршрутизации с одинаковым значением веса поведение не определено, то есть неизвестно, какая таблица будет использоваться в первую очередь.

Форма **set** данной команды используется для определения таблицы маршрутизации в качестве резервной.

Форма **delete** используется для отмены использования таблицы маршрутизации в качестве резервной.

Форма **show** используется для отображения текущего значения параметра.

32.3.13 policy route <имя_политики> rule <номер_правила> table <имя_таблицы> weight <вес_таблицы>

Указание веса определённой таблицы маршрутизации.

Синтаксис

```
set policy route <имя_политики>и rule <номер_правила> table <имя_таблицы> weight <вес_таблицы>
```

```
delete policy route <имя_политики> rule <номер_правила> table <имя_таблицы> weight <вес_таблицы>
```

```
show policy route <имя_политики> rule <номер_правила> table <имя_таблицы> weight <вес_таблицы>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route имя_политики {
        rule номер_правила {
            table имя_таблицы {
                weight вес_таблицы
            }
        }
    }
}
```

Параметры

имя_политики

Имя политики маршрутизации трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 65535. В том случае если необходимо определить

несколько правил, следует создать соответствующее количество узлов конфигурации rule.

имя_таблицы

Имя таблицы маршрутизации трафика.

вес_таблицы

Вес таблицы маршрутизации. Значение должно лежать в диапазоне от 1 до 65535.

Значение по умолчанию

По умолчанию вес таблиц равен 1.

Указания по использованию

Данная команда указывает вес определённой таблицы маршрутизации для данной политики маршрутизации трафика. Вероятность выбора данной таблицы в рамках правила политики маршрутизации пропорциональна указанному значению веса. При наличии нескольких таблиц маршрутизации с одинаковым значением веса, вероятность выбора таблицы пропорционально делится на количество таблиц. (Например при наличии двух таблиц с одинаковым весом, вероятность выбора каждой из них равна 50%, четырёх — 25%).

Для резервных (failover) таблиц значение веса определяет последовательность выбора таблиц в рамках политики маршрутизации при наличии в системе двух и более резервных таблиц.

Форма **set** указания значения веса таблицы маршрутизации.

Форма **delete** установки значения по умолчанию

Форма **show** используется для отображения текущего значения.

32.3.14 policy route-ipv6 <имя_политики>

Определение политики маршрутизации трафика IPv6.

Синтаксис

```
set policy route-ipv6 <имя_политики>
delete policy route-ipv6 <имя_политики>
show policy route-ipv6 <имя_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route-ipv6 имя_политики {
   }
}
```

Параметры

имя_политики

Множественный узел. Текстовый идентификатор политики маршрутизации трафика IPv6.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания политики маршрутизации трафика.

Форма **delete** этой команды используется для удаления политики маршрутизации трафика.

Форма **show** этой команды используется для отображения настройки политики маршрутизации трафика.

32.3.15 policy route-ipv6 <имя_политики> description <описание>

Создание текстового описания для указанной политики маршрутизации трафика IPv6.

Синтаксис

```
set policy route-ipv6 <имя_политики> description <описание>
delete policy route-ipv6 <имя_политики> description
show policy route-ipv6 <имя_политики> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route-ipv6 имя_политики {
      description описание
   }
}
```

Параметры

имя_политики

Имя политики маршрутизации трафика IPv6.

описание

Текстовое описание политики. В том случае если описание содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма set данной команды используется для задания текстового описания для указанной политики.

Форма delete используется для удаления описания.

Форма show используется для отображения описания.

32.3.16 policy route-ipv6 <имя_политики> flow-balancing <состояние>

Включение или отключение балансировки соединений для данной политики маршрутизации трафика IPv6.

Синтаксис

```
set policy route-ipv6 <имя_политики> flow-balancing <состояние>
delete policy route-ipv6 <имя_политики> flow-balancing
show policy route-ipv6 <имя_политики> flow-balancing
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route-ipv6 имя_политики {
      flow-balancing состояние
   }
}
```

Параметры

имя_политики

Множественный узел. Текстовый идентификатор политики маршрутизации трафика IPv6.

состояние

Указатель режима работы балансировки соединений. Допустимые значения:

enable: Балансировка соединений включена.

disable: Балансировка соединений отключена.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать режим балансировки соединений вместо пакетов для политики маршрутизации трафика IPv6.

Форма **set** этой команды используется для указания режима работы балансировки соединений.

Форма **delete** этой команды используется для удаления указанного режима работы балансировки соединений.

Форма **show** этой команды используется для отображения настройки балансировки соединений.

32.3.17 policy route-ipv6 <имя_политики> rule <номер_правила>

Создание правила для политики маршрутизации трафика IPv6.

Синтаксис

```
set policy route-ipv6 <имя_политики> rule <номер_правила>
delete policy route-ipv6 <имя_политики> rule <номер_правила>
show policy route-ipv6 <имя_политики> rule <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route-ipv6 имя_политики {
      rule номер_правила {
      }
   }
}
```

Параметры

имя_политики

Множественный узел. Текстовый идентификатор политики маршрутизации трафика IPv6.

номер_правила

Множественный узел. Численный идентификатор правила. Значение должно лежать в диапазоне 1-65535.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для создания правила для политики маршрутизации трафика.

Форма **delete** этой команды используется для удаления правила для политики маршрутизации трафика.

Форма **show** этой команды используется для отображения параметров настройки правила политики маршрутизации трафика.

32.3.18 policy route-ipv6 <имя_политики> rule <номер_правила> description <описание>

Задание текстового описания для правила в указанной политики маршрутизации трафика IPv6.

Синтаксис

```
set policy route-ipv6 <имя_политики> rule <номер_правила> description
<описание>
delete policy route-ipv6 <имя_политики> rule <номер_правила> description
show policy route-ipv6 <имя_политики> rule <номер_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route-ipv6 имя_политики {
      rule номер_правила {
         description описание
      }
   }
}
```

Параметры

имя_политики

Имя политики маршрутизации трафика IPv6.

описание

Текстовое описание политики. В том случае если описание содержит пробелы, его необходимо заключить в двойные кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для задания текстового описания для указанной политики.

Форма **delete** используется для удаления описания.

Форма **show** используется для отображения описания.

32.3.19 policy route-ipv6 <имя_политики> rule <номер_правила> log <состояние>

Включение или отключение протоколирования правила данной политики маршрутизации трафика IPv6.

Синтаксис

```
set policy route-ipv6 <имя_политики> rule <номер_правила> log <состояние>
delete policy route-ipv6 <имя_политики> rule <номер_правила>
show policy route-ipv6 <имя_политики> rule <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   route-ipv6 имя_политики {
      rule номер_правила {
         log состояние
      }
   }
}
```

Параметры

имя_политики

Множественный узел. Текстовый идентификатор политики маршрутизации трафика.

номер_правила

Множественный узел. Численный идентификатор правила.

состояние

Указатель режима протоколирования правила политики. Допустимые значения:

enable: Протоколирование правила политики включено.

disable: Протоколирование правила политики отключено.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для указания режима протоколирования правила политики маршрутизации трафика.

Форма **delete** этой команды используется для удаления указанного режима протоколирования правила политики маршрутизации трафика.

Форма **show** этой команды используется для отображения настройки режима протоколирования правила политики маршрутизации трафика.

32.3.20 policy route-ipv6 <имя_политики> rule <номер_правила> match filter-ipv6 <имя_фильтра>

Указание применения определённого фильтра трафика IPv6 для данной политики маршрутизации трафика IPv6.

Синтаксис

```
set policy route-ipv6 <имя_политики> rule <номер_правила> match filter-ipv6 <имя_фильтра>

delete policy route-ipv6 <имя_политики> rule <номер_правила> match filter-ipv6

show policy route-ipv6 <имя_политики> rule <номер_правила> match filter-ipv6
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-ipv6 имя_политики {
        rule номер_правила {
            match filter-ipv6 имя_фильтра
        }
    }
}
```

Параметры

имя_политики

Множественный узел. Текстовый идентификатор политики маршрутизации трафика IPv6.

номер_правила

Множественный узел. Численный идентификатор правила.

имя_фильтра

Текстовый формат. Название фильтра трафика IPv6, который будет применен для данной политики маршрутизации трафика IPv6.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для указания применения определенного фильтра трафика для данной политики маршрутизации трафика.

Форма **delete** этой команды используется для удаления указанного фильтра трафика для данной политики маршрутизации трафика.

Форма **show** этой команды используется для отображения настройки применения фильтров трафика к данной политике маршрутизации трафика.

32.3.21 policy route-ipv6 <имя_политики> rule <номер_правила> table <имя_таблицы>

Указание применения определённой таблицы маршрутизации для данной политики маршрутизации трафика IPv6.

Синтаксис

```
set policy route-ipv6 <имя_политики> rule <номер_правила> table <имя_таблицы>
```

```
delete policy route-ipv6 <имя_политики> rule <номер_правила> table <имя_таблицы>
```

```
show policy route-ipv6 <имя_политики> rule <номер_правила> table <имя_таблицы>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-ipv6 имя_политики {
        rule номер_правила {
            table имя_таблицы {
            }
        }
    }
}
```

Параметры

имя_политики

Множественный узел. Текстовый идентификатор политики маршрутизации трафика IPv6.

номер_правила

Множественный узел. Численный идентификатор правила.

имя_таблицы

Текстовый формат. Название таблицы маршрутизации, которая будет применена для данной политики маршрутизации трафика IPv6.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для указания таблицы маршрутизации для данной политики маршрутизации трафика.

Форма **delete** этой команды используется для удаления указанной таблицы маршрутизации для данной политики маршрутизации трафика.

Форма **show** этой команды используется для отображения настройки использования таблиц маршрутизации для данной политики маршрутизации трафика.

32.3.22 policy route-ipv6 <имя_политики> rule <номер_правила> table <имя_таблицы> failover-table

Использовать определённую таблицу маршрутизации только если другие таблицы недоступны.

Синтаксис

```
set policy route-ipv6 <имя_политики> rule <номер_правила> table <имя_таблицы> failover-table

delete policy route-ipv6 <имя_политики> rule <номер_правила> table <имя_таблицы> failover-table

show policy route-ipv6 <имя_политики> rule <номер_правила> table <имя_таблицы>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-ipv6 имя_политики {
        rule номер_правила {
            table имя_таблицы {
                failover-table
            }
        }
    }
}
```

Параметры

имя_политики

Множественный узел. Текстовый идентификатор политики маршрутизации трафика IPv6.

номер_правила

Множественный узел. Численный идентификатор правила.

имя_таблицы

Текстовый формат. Название таблицы маршрутизации, которая будет применена для данной политики маршрутизации трафика IPv6.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда устанавливает режим работы, при котором указанная таблица маршрутизации используется только в том случае если другие таблицы недоступны.

Форма **set** этой команды используется для указания режима использовать определённую таблицу маршрутизации только если другие таблицы недоступны.

Форма **delete** этой команды используется для удаления указания режима использовать определённую таблицу маршрутизации только если другие таблицы недоступны.

Форма **show** этой команды используется для отображения настройки использования таблиц маршрутизации для данной политики маршрутизации трафика.

32.3.23 policy route-ipv6 <имя_политики> rule <номер_правила> table <имя_таблицы> weight <вес>

Указание веса определённой таблицы маршрутизации.

Синтаксис

```
set policy route-ipv6 <имя_политики> rule <номер_правила> table <имя_таблицы> weight <вес>

delete policy route-ipv6 <имя_политики> rule <номер_правила> table <имя_таблицы> weight

show policy route-ipv6 <имя_политики> rule <номер_правила> table <имя_таблицы> weight
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    route-ipv6 имя_политики {
        rule номер_правила {
            table имя_таблицы {
                weight вес
            }
        }
    }
}
```

Параметры

имя_политики

Множественный узел. Текстовый идентификатор политики маршрутизации трафика IPv6.

номер_правила

Множественный узел. Численный идентификатор правила.

имя_таблицы

Текстовый формат. Название таблицы маршрутизации, которая будет применена для данной политики маршрутизации трафика IPv6.

вес

Устанавливает вес определенной таблицы маршрутизации. Параметр используется для расстановки приоритетов между несколькими таблицами маршрутизации. Значение должно лежать в диапазоне 1-65535.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для указания веса таблицы маршрутизации для данной политики маршрутизации трафика.

Форма **delete** этой команды используется для удаления веса таблицы маршрутизации для данной политики маршрутизации трафика.

Форма **show** этой команды используется для отображения настройки веса таблицы маршрутизации для данной политики маршрутизации трафика.

32.3.24 policy clear route <имя_политики>

Очистка статистики политики маршрутизации трафика.

Синтаксис

```
policy clear route <имя_политики>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики маршрутизации трафика.

Значение по умолчанию

Отсутствует.

32.3.25 policy clear route <имя_политики> rule <номер_правила>

Очистка статистики правила политики маршрутизации.

Синтаксис

```
policy clear route <имя_политики> rule <номер_правила>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики маршрутизации трафика.

номер_правила

Множественный узел. Численный идентификатор правила.

Значение по умолчанию

Отсутствует.

32.3.26 policy clear route <имя_политики> rule <номер_правила> filter

Очистка статистики для фильтра, связанного с указанным правилом политики маршрутизации.

Синтаксис

```
policy clear route <имя_политики> rule <номер_правила> filter
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики маршрутизации трафика.

номер_правила

Множественный узел. Численный идентификатор правила.

Значение по умолчанию

Отсутствует.

32.3.27 policy clear route <имя_политики> rule <номер_правила> filter rule <номер_правила>

Очистка статистики по указанному правилу фильтра, связанного с указанным правилом политики маршрутизации.

Синтаксис

```
policy clear route <имя_политики> rule <номер_правила> filter <номер_правила>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики маршрутизации трафика.

rule *номер_правила*

Множественный узел. Численный идентификатор правила.

filter rule *номер_правила*

Множественный узел. Численный идентификатор правила фильтра.

Значение по умолчанию

Отсутствует.

32.3.28 policy show route <имя_политики>

Вывод сведений и статистики для указанной политики маршрутизации.

Синтаксис

```
policy show route <имя_политики>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики маршрутизации трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отображения сведений о выбранной настроенной политике маршрутизации.

32.3.29 policy show route <имя_политики> rule <номер_правила>

Вывод конфигурации правила политики маршрутизации.

Синтаксис

```
policy show <имя_политики> rule <номер_правила>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики маршрутизации трафика.

номер_правила

Множественный узел. Численный идентификатор правила.

Значение по умолчанию

Отсутствует.

32.3.30 policy show route <имя_политики> rule <номер_правила> filter

Вывод сведений о фильтре, связанному с указанным правилом.

Синтаксис

```
policy show route <имя_политики> rule <номер_правила> filter [detail]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики маршрутизации трафика.

номер_правила

Множественный узел. Численный идентификатор правила.

detail

Вывои подробных сведения о примененном фильтре.

Значение по умолчанию

Отсутствует.

Примеры

В примере приведен образец вывода подробных сведений о конфигурации и статистики по указанному правилу политики маршрутизации и фильтрам, связанным с ним.

Пример 310 – Вывод подробных сведений о конфигурации и статистики для отдельного правила политики маршрутизации и фильтру, связанному с ним.

```
admin@edge01:~$ policy show route test rule 10 filter detail
Фильтр IPv4 test:

 Фильтр задействован для политик маршрутизации трафика: (test: 10)


rule      pkts      bytes     source              destination         proto
state
----      ----      -----     ------              -----------         -----
-----
10        0         0         0.0.0.0/0           192.168.200.0/24    all
any
```

32.3.31 policy show route <имя_политики> rule <номер_правила> filter rule <номер_правила>

Вывод статистики по указанному правилу фильтра, связанного с указанным правилом политики маршрутизации.

Синтаксис

```
policy show route <имя_политики> rule <номер_правила> filter rule
<номер_правила>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики маршрутизации трафика.

rule *номер_правила*

Множественный узел. Численный идентификатор правила.

filter rule *номер_правила*

Множественный узел. Численный идентификатор правила фильтра.

Значение по умолчанию

Отсутствует.

33 Политика клонирования трафика

В этом разделе даны указания по настройке политик клонирования трафика на системе Numa Edge.

Рассматриваются следующие вопросы:

- Обзор политик клонирования трафика.
- Пример настройки политик клонирования трафика.
- Команды политик клонирования трафика.

33.1 Обзор политик клонирования трафика

Политики клонирования трафика — это механизм, позволяющий копировать (клонировать) пакеты, которые соответствуют критериям определённого фильтра, а именно копировать (или клонировать) пакеты, соответствующие критериям определённого фильтра, на удаленный шлюз.

В настройках Numa Edge политики клонирования трафика сгруппированы узлами **policy clone** и **policy clone-ipv6**, которые служат контейнерами для операторов политики. Действующими операторами политики определяются правила клонирования трафика. При этом клонирование трафика согласно определённой политике производится только в случае её применения к конкретному интерфейсу.

Политики клонирования трафика применяются первыми после получения данных перед применением правил МЭ и политик модификации трафика, как показано на рисунке ниже

33.2 Пример настройки политик клонирования трафика

В данном разделе приведен пример настройки для политики клонирования трафика.

Пример рассматривает настройку политики клонирования входящего на интерфейсе Ethernet eth0 по протоколу IPv4 на шлюз 192.168.23.3

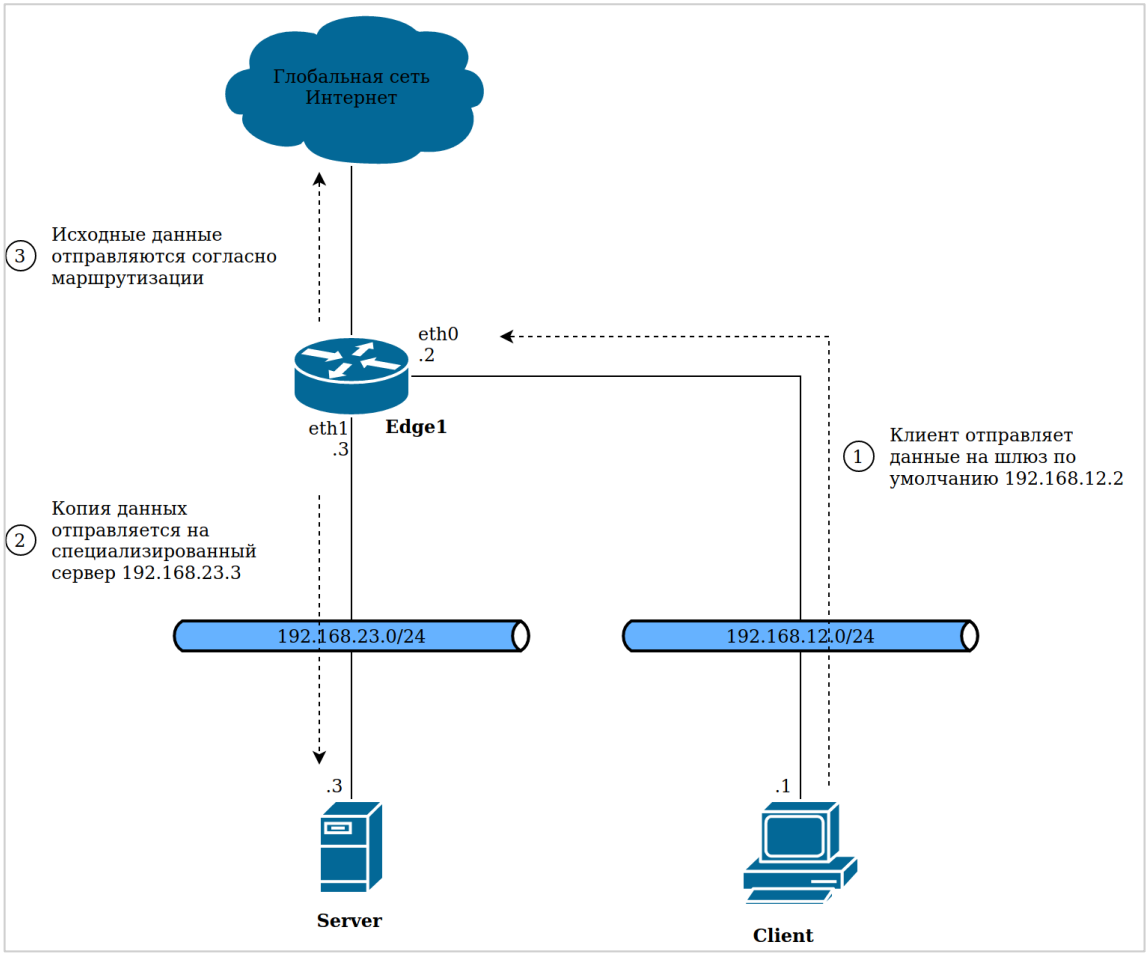


Рисунок 77 – Схема стенда

33.2.1 Пример настройки политики клонирования входящего IGMP-трафика

- Создаётся фильтр для трафика.
- Создаётся политика клонирования пакетов, атрибуты которых соответствуют определённому фильтру, на шлюз 192.168.23.3.

Пример 311 - Пример настройки политики клонирования входящего трафика.

Действие	**Команда**
Создание фильтра.	`[edit]` `admin@edge# set filter Input_IPv4_traffic`
Установка описания для созданного фильтра.	`[edit]` `admin@edge# set filter Input_IPv4_traffic description "All ipv4 input traffic"`
Создание правила для фильтра для определения входящего трафика.	`admin@edge# set filter Input_IPv4_traffic rule 10 protocol all`
Фиксация изменений.	`[edit]` `admin@edge# commit`

Вывод настройки фильтра.	`[edit]`
	`admin@edge# show filter`
	`Input_IPv4_traffic {`
	`description "All ipv4 input traffic"`
	`rule 10 {`
	`protocol all`
	`}`
	`}`

Действие	**Команда**
Указание использования определённого фильтра трафика для правила политики клонирования трафика с именем **Clone_IPv4_traffic**.	[edit] admin@edge# set policy clone Clone_IPv4_traffic rule 10 match filter Input_IPv4_traffic
Указание шлюза с IP-адресом 192.168.23.3, в качестве шлюза, на который будет происходить клонирование трафика атрибуты которого совпадают с определённым фильтром.	[edit] admin@edge# set policy clone Clone_IPv4_traffic rule 10 gateway-addr 192.168.23.3
Фиксация изменений.	[edit] admin@edge# commit

Вывод правила клонирования трафика.	[edit]
	admin@edge# show policy clone Clone_IPv4_traffic
	rule 10 {
	gateway-addr 192.168.23.3
	match {
	filter Input_IPv4_traffic
	}
	}

Применение политики клонирования трафика для входящего IPv4-трафика на интерфейсе Ethernet eth0.	[edit] admin@edge# set interfaces ethernet eth0 policy in clone Clone_IPv4_traffic
Фиксация изменений.	[edit] admin@edge# commit

Вывод применённых политик клонирования входящего IPv4-трафика для интерфейса Ethernet eth0.	[edit]
	admin@edge# show interfaces ethernet eth0
	address 192.168.12.2/24
	policy {
	in {
	clone Clone_IPv4_traffic
	}
	}

33.3 Команды политик клонирования трафика

В данном разделе приведены команды для настройки политик клонирования трафика.

Таблица 268 - Команды настройки политик клонирования трафика.

Режим настройки	
Применение политик клонирования IPv4-трафика к интерфейсам	
interfaces <интерфейс> policy in clone <имя_политики>	Применение политики клонирования IPv4-трафика к указанному интерфейсу.
Применение политик клонирования IPv6-трафика к интерфейсам	
interfaces <интерфейс> policy in clone-ipv6 <имя_политики>	Применение политики клонирования IPv6-трафика к указанному интерфейсу.
Команды клонирования трафика для протокола IPv4	
policy clone <имя_политики>	Указание имени политики клонирования IPv4-трафика.
policy clone <имя_политики> rule <номер_правила> gateway-addr <ipv4-адрес>	Указание IPv4-адреса шлюза, на который будет происходить клонирование трафика.
policy clone <имя_политики> rule <номер_правила> log <состояние>	Включение/выключение регистрации событий клонирования для указанного правила указанной политики клонирования IPv4.
policy clone <имя_политики> rule <номер_правила> match filter <название_фильтра>	Указание применения определённого фильтра трафика для правила данной политики клонирования IPv4-трафика.
Команды клонирования трафика для протокола IPv6	

policy clone-ipv6 <имя_политики>	Указание имени политики клонирования IPv6-трафика.
policy clone-ipv6 <имя_политики> rule <номер_правила> gateway-addr <ipv6_адрес>	Указание IPv6-адреса шлюза, на который будет происходить клонирование трафика.
policy clone-ipv6 <имя_политики> rule <номер_правила> log <состояние>	Включение/выключение регистрации событий клонирования для указанного правила указанной политики клонирования IPv6.
policy clone-ipv6 <имя_политики> rule <номер_правила> match filter <название_фильтра>	Указание применения определённого фильтра трафика для правила данной политики клонирования IPv6-трафика.
Эксплуатационные команды IPv4	
policy clear clone <имя_политики>	Очистка статистики политики клонирования IPv4-трафика.
policy clear clone <имя_политики> rule <номер_правила>	Очистка статистики для указанного правила политики клонирования IPv4-трафика.
policy clear clone <имя_политики> rule <номер_правила> filter	Очистка статистики для фильтра, связанного с указанным правилом политики клонирования IPv4-трафика.
policy clear clone <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>	Очистка статистики по указанному правилу фильтра, связанного с указанным правилом политики клонирования IPv4-трафика.
policy show clone <имя_политики>	Вывод сведений и статистики для указанной политики клонирования IPv4-трафика.
policy show clone <имя_политики> rule <номер_правила>	Вывод конфигурации для указанного правила политики клонирования IPv4-трафика.
policy show clone <имя_политики> rule <номер_правила> filter	Вывод подробных сведений о конфигурации и статистики по указанному правилу политики клонирования IPv4-трафика и фильтру, связанному с ним.
policy show clone <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>	Вывод статистики по указанному правилу фильтра, связанного с указанным правилом политики клонирования IPv4-трафика.
Эксплуатационные команды IPv6	
policy clear clone-ipv6 <имя_политики>	Очистка статистики политики клонирования IPv6-трафика.
policy clear clone-ipv6 <имя_политики> rule <номер_правила>	Очистка статистики для указанного правила политики клонирования IPv6-трафика.
policyclearclone-ipv6 <имя_политики> rule <номер_правила> filter	Очистка статистики для фильтра, связанного с указанным правилом политики клонирования IPv6-трафика.
policy clear clone-ipv6 <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>	Очистка статистики по указанному правилу фильтра, связанного с указанным правилом политики клонирования IPv6-трафика.
policy show clone-ipv6 <имя_политики>	Вывод сведений и статистики для указанной политики клонирования IPv6-трафика.
policy show clone-ipv6 <имя_политики> rule <номер_правила>	Вывод конфигурации правила политики клонирования IPv6-трафика.
policy show clone-ipv6 <имя_политики> rule <номер_правила> filter	Вывод подробных сведений о конфигурации и статистики по указанному правилу политики клонирования IPv6-трафика и фильтру, связанному с ним.
policy show clone-ipv6 <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>	Вывод статистики по указанному правилу фильтра, связанного с указанным правилом политики клонирования IPv6-трафика.

33.3.1 interfaces <интерфейс> policy in clone <имя_политики>

Применение политики клонирования IPv4-трафика к указанному интерфейсу.

Синтаксис

```
set interfaces <интерфейс> policy in clone <имя_политики>
delete interfaces <интерфейс> policy in clone
```

```
show interfaces <интерфейс> policy in clone
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
   policy {
      in {
         clone имя_политики
      }
   }
}
```

Параметры

интерфейс

Интерфейс, к которому применяется политика клонирования трафика. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже в разделе Указания по использованию.

имя_политики

Имя политики клонирования трафика, применяемой к данному интерфейсу.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для применения политики клонирования IPv4-трафика к интерфейсу.

В приведенной ниже таблице показаны типы поддерживаемых интерфейсов и синтаксис.

Таблица 269 – Типы интерфейсов

Тип интерфейса	Синтаксис
Агрегирование каналов	bonding bondx
Виртуальный интерфейс агрегированных каналов	bonding bondx vif идентификатор_vlan
Сетевой мост	bridge brx
Ethernet	ethernet ethx
Ethernet PPPoE	ethernet ethx pppoe номер
Виртуальный интерфейс Ethernet	ethernet ethx vif идентификатор_vlan
Ethernet Vif PPPoE	ethernet ethx vif идентификатор_vlan pppoe номер
Интерфейс заглушки	loopback lo
Многоканальная связь	multilink mlx
OpenVPN	openvpn vtunx
Псевдо-Ethernet	pseudo-ethernet pethx
Последовательный интерфейс	serial srx vif идентификатор_vlan
Туннель	tunnel tunx

Форма **set** этой команды используется для применения политики клонирования трафика к интерфейсу.

Форма **delete** этой команды используется для удаления политики клонирования трафика с интерфейса.

Форма **show** этой команды используется для отображения настройки политики клонирования трафика на интерфейсе.

33.3.2 interfaces <интерфейс> policy in clone-ipv6 <имя_политики>

Применение политики клонирования IPv6-трафика к указанному интерфейсу.

Синтаксис

```
set interfaces <интерфейс> policy in clone-ipv6 <имя_политики>
delete interfaces <интерфейс> policy in clone-ipv6
show interfaces <интерфейс> policy in clone-ipv6
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces интерфейс {
   policy {
      in {
         clone-ipv6 имя_политики
      }
   }
}
```

Параметры

интерфейс

Интерфейс, к которому применяется политика клонирования трафика. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже в разделе Указания по использованию.

имя_политики

Имя политики клонирования трафика IPv6, применяемой к данному интерфейсу.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для применения политики клонирования IPv6-трафика к интерфейсу.

В приведенной ниже таблице показаны типы поддерживаемых интерфейсов и синтаксис.

Таблица 270 – Типы интерфейсов

Тип интерфейса	Синтаксис
Агрегирование каналов	bonding bondx
Виртуальный интерфейс агрегированных каналов	bonding bondx vif идентификатор_vlan
Сетевой мост	bridge brx
Ethernet	ethernet ethx
Ethernet PPPoE	ethernet ethx pppoe номер
Виртуальный интерфейс Ethernet	ethernet ethx vif идентификатор_vlan
Ethernet Vif PPPoE	ethernet ethx vif идентификатор_vlan pppoe номер
Интерфейс заглушки	loopback lo
Многоканальная связь	multilink mlx
OpenVPN	openvpn vtunx
Псевдо-Ethernet	pseudo-ethernet pethx
Последовательный интерфейс	serial srx vif идентификатор_vlan
Туннель	tunnel tunx

Форма **set** этой команды используется для применения политики клонирования трафика к интерфейсу.

Форма **delete** этой команды используется для удаления политики клонирования с интерфейса.

Форма **show** этой команды используется для отображения настройки политики клонирования трафика на интерфейсе.

33.3.3 policy clone <имя_политики>

Указание имени политики клонирования IPv4-трафика.

Синтаксис

```
set policy clone <имя_политики>
delete policy clone <имя_политики>
show policy clone <имя_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    clone имя_политики {
    }
}
```

Параметры

имя_политики

Имя определённой политики клонирования IPv4-трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для определения политики клонирования трафика.

Форма **delete** этой команды используется для удаления политики клонирования трафика.

Форма **show** этой команды используется для удаления политики клонирования трафика.

33.3.4 policy clone <имя_политики> rule <номер_правила> gateway-addr <ipv4-адрес>

Указание IPv4-адреса шлюза, на который будет происходить клонирование трафика.

Синтаксис

```
set policy clone <имя_политики> rule <номер_правила> gateway-addr <ipv4-адрес>
delete policy clone <имя_политики> rule <номер_правила> match <ipv4-адрес>
show policy clone <имя_политики> rule <номер_правила> match
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    clone имя_политики {
        rule номер_правила {
            gateway-addr ipv4-адрес
        }
    }
}
```

Параметры

имя_политики

Имя определённой политики клонирования IPv4-трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 9999. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

ipv4-адрес

IPv4-адрес шлюза, на который будет происходить клонирование трафика. Для указания адреса используется стандартный формат IPv4-адреса x.x.x.x (например, 192.168.23.3).

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для определения адреса шлюза, на который будет клонироваться входящий IPv4-трафик, атрибуты которого соответствую определённому фильтру.

Форма **delete** этой команды используется для удаления адреса шлюза.

Форма **show** этой команды используется для удаления адреса шлюза.

33.3.5 policy clone <имя_политики> rule <номер_правила> log <состояние>

Включение/выключение регистрации событий клонирования для указанного правила указанной политики клонирования IPv4.

Синтаксис

```
set policy clone <имя_политики> rule <номер_правила> log <состояние>
delete policy clone <имя_политики> rule <номер_правила> log
show policy clone <имя_политики> rule <номер_правила> log
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   clone имя_политики {
      rule номер_правила {
         log состояние
      }
   }
}
```

Параметры

имя_политики

Имя определённой политики клонирования IPv4-трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 9999. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

состояние

Для настройки регистрации событий клонирования для правила политики следует указать одно из двух ключевых слов:

enable – включить регистрацию;

disable – отключить регистрацию.

Значение по умолчанию

Отсутствует.

Указания по использованию

В том случае, если задействовано журналирование для правила политики, в системный лог (журнал) будут выводиться сообщения для всех пакетов, подпадающих под правило. Для каждого сообщения формируется префикс в квадратных скобках ([c-<имя_политики>-<номер_правила>]). Имя политики может быть записано в журнале не полностью в связи с системным ограничением общей длины префикса в 29 символов.

Форма **set** этой команды используется для задания настройки регистрации событий клонирования для указанного правила указанной политики.

Форма **delete** этой команды используется для удаления настройки регистрации событий клонирования.

Форма **show** этой команды используется для отображения настройки регистрации событий клонирования.

33.3.6 policy clone <имя_политики> rule <номер_правила> match filter <название_фильтра>

Указание применения определённого фильтра трафика для правила данной политики клонирования IPv4-трафика.

Синтаксис

```
set policy clone <имя_политики> rule <номер_правила> match <название_фильтра>
delete policy clone <имя_политики> rule <номер_правила> match <название_фильтра>
show policy clone <имя_политики> rule <номер_правила> match <название_фильтра>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    clone имя_политики {
        rule номер_правила {
            match {
                filter название_фильтра
            }
        }
    }
}
```

Параметры

имя_политики

Имя определённой политики клонирования IPv4-трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 9999. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

название_фильтра

Название фильтра IPv4-трафика. Фильтр должен быть заранее определен в системе.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для определения условия соответствия, основанного на определённом фильтре.

Форма **delete** этой команды используется для удаления условия соответствия трафика.

Форма **show** этой команды используется для отображения настройки условия соответствия трафика.

33.3.7 policy clone-ipv6 <имя_политики>

Указание имени политики клонирования IPv6-трафика.

Синтаксис

```
set policy clone-ipv6 <имя_политики>
delete policy clone-ipv6 <имя_политики>
show policy clone-ipv6 <имя_политики>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
   clone-ipv6 имя_политики {
   }
}
```

Параметры

имя_политики

Имя определённой политики клонирования IPv6-трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для определения политики клонирования трафика.

Форма **delete** этой команды используется для удаления политики клонирования трафика.

Форма **show** этой команды используется для удаления политики клонирования трафика.

33.3.8 policy clone-ipv6 <имя_политики> rule <номер_правила> gateway-addr <ipv6_адрес>

Указание IPv6-адреса шлюза, на который будет происходить клонирование трафика.

Синтаксис

```
set policy clone-ipv6 <имя_политики> rule <номер_правила> gateway-addr
<ipv6_адрес>
delete policy clone-ipv6 <имя_политики> rule <номер_правила> gateway-addr
show policy clone-ipv6 <имя_политики> rule <номер_правила> gateway-addr
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
```

```
    clone-ipv6 имя_политики {
        rule номер_правила {
            gateway-addr ipv6_адрес
        }
    }
}
```

Параметры

имя_политики

Имя определённой политики клонирования IPv6-трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 9999. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

ipv6_адрес

IPv6-адрес шлюза, на который будет происходить клонирование трафика. Для указания адреса используется стандартный формат IPv6-адреса <x:x:x:x:x:x:x:x> IP-адрес (например, fc00::23:3).

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для определения адреса шлюза, на который будет клонироваться входящий IPv6-трафик, атрибуты которого соответствую определённому фильтру.

Форма **delete** этой команды используется для удаления адреса шлюза.

Форма **show** этой команды используется для удаления адреса шлюза.

33.3.9 policy clone-ipv6 <имя_политики> rule <номер_правила> log <состояние>

Включение/выключение регистрации событий клонирования для указанного правила указанной политики клонирования IPv6.

Синтаксис

```
set policy clone-ipv6 <имя_политики> rule <номер_правила> log <состояние>
delete policy clone-ipv6 <имя_политики> rule <номер_правила> log
show policy clone-ipv6 <имя_политики> rule <номер_правила> log
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    clone-ipv6 имя_политики {
        rule номер_правила {
            log состояние
        }
    }
}
```

Параметры

имя_политики

Имя определённой политики клонирования IPv4-трафика.

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 9999. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации rule.

состояние

Для настройки регистрации событий клонирования для правила политики следует указать одно из двух ключевых слов:

enable – включить регистрацию;

disable – отключить регистрацию.

Значение по умолчанию

Отсутствует.

Указания по использованию

В том случае, если задействовано журналирование для правила политики, в системный лог (журнал) будут выводиться сообщения для всех пакетов, подпадающих под правило. Для каждого сообщения формируется префикс в квадратных скобках ([c6-<имя_политики>-<номер правила>]). Имя политики может быть записано в журнале не полностью в связи с системным ограничением общей длины префикса в 29 символов.

Форма **set** этой команды используется для задания настройки регистрации событий клонирования для указанного правила указанной политики.

Форма **delete** этой команды используется для удаления настройки регистрации событий клонирования.

Форма **show** этой команды используется для отображения настройки регистрации событий клонирования.

33.3.10 policy clone-ipv6 <имя_политики> rule <номер_правила> match filter <название_фильтра>

Указание применения определённого фильтра трафика для правила данной политики клонирования IPv6-трафика.

Синтаксис

```
set policy clone-ipv6 <имя_политики> rule <номер_правила> match <название_фильтра>

delete policy clone-ipv6 <имя_политики> rule <номер_правила> match <название_фильтра>

show policy clone-ipv6 <имя_политики> rule <номер_правила> match <название_фильтра>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
policy {
    clone-ipv6 имя_политики {
        rule номер_правила {
            match {
                filter название_фильтра
            }
        }
    }
}
```

Параметры

имя_политики

Имя определённой политики клонирования IPv6-трафика.

номер_правила

Номер определенного правила политики клонирования IPv6-трафика.

название_фильтра

Название определённого фильтра IPv6-трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для определения условия соответствия, основанного на определённом фильтре.

Форма **delete** этой команды используется для удаления условия соответствия трафика.

Форма **show** этой команды используется для отображения настройки условия соответствия трафика.

33.3.11 policy clear clone <имя_политики>

Очистка статистики политики клонирования IPv4-трафика.

Синтаксис

```
policy clear clone <имя_политики>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики клонирования IPv4-трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отчистки статистики клонирования IPv4-трафика для указанной политики.

33.3.12 policy clear clone <имя_политики> rule <номер_правила>

Очистка статистики правила политики клонирования IPv4-трафика.

Синтаксис

```
policy clear clone <имя_политики> rule <номер_правила>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики клонирования IPv4-трафика.

номер_правила

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999. Если необходимо очистить статистику для нескольких правил, следует применить команду clear к каждому из них в отдельности.

Значение по умолчанию

Отсутствует.

33.3.13 policy clear clone <имя_политики> rule <номер_правила> filter

Очистка статистики для фильтра, связанного с указанным правилом политики клонирования IPv4-трафика.

Синтаксис

```
policy clear clone <имя_политики> rule <номер_правила> filter
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики клонирования IPv4-трафика.

номер_правила

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

Значение по умолчанию

Отсутствует.

33.3.14 policy clear clone <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>

Очистка статистики по указанному правилу фильтра, связанного с указанным правилом политики клонирования IPv4-трафика.

Синтаксис

```
policy clear clone <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики клонирования IPv4-трафика.

номер_правила

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

номер_правила_фильтра

Численный идентификатор правила фильтра. Значение должно лежать в диапазоне от 1 до 9999.

Значение по умолчанию

Отсутствует.

33.3.15 policy show clone <имя_политики>

Вывод сведений и статистики для указанной политики клонирования IPv4-трафика.

Синтаксис

```
policy show clone <имя_политики>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики клонирования IPv4-трафика.

Значение по умолчанию

При использовании без параметров отображается сводка для всех политик клонирования IPv4-трафика.

Указания по использованию

Эта команда используется для отображения сведений о выбранной настроенной политике клонирования IPv4-трафика.

Сведения об интерфейсах, к которым применена указанная политика, не выводятся. Для просмотра сведений о политиках клонирования IPv4-трафика, примененных к конкретному интерфейсу, следует применять команду **show interfaces** для интерфейса.

33.3.16 policy show clone <имя_политики> rule <номер_правила>

Вывод конфигурации правила политики клонирования IPv4-трафика.

Синтаксис

policy show clone <имя_политики> rule <номер_правила>

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики клонирования IPv4-трафика.

номер_правила

Численный идентификатор правила.

Значение по умолчанию

Отсутствует.

33.3.17 policy show clone <имя_политики> rule <номер_правила> filter

Вывод сведений о конфигурации и статистики по указанному правилу политики клонирования IPv4-трафика и фильтру, связанному с ним.

Синтаксис

policy show clone <имя_политики> rule <номер_правила> filter [detail]

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики клонирования IPv4-трафика.

номер_правила

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

detail

Вывод подробных сведений о конфигурации и статистике.

Значение по умолчанию

Отсутствует.

33.3.18 policy show clone <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>

Вывод статистики по указанному правилу фильтра, связанного с указанным правилом политики клонирования IPv4-трафика.

Синтаксис

```
policy show clone <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики клонирования IPv4-трафика.

номер_правила

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

номер_правила_фильтра

Численный идентификатор правила фильтра. Значение должно лежать в диапазоне от 1 до 9999.

Значение по умолчанию

Отсутствует.

33.3.19 policy clear clone-ipv6 <имя_политики>

Очистка статистики политики клонирования IPv6-трафика.

Синтаксис

```
policy clear clone-ipv6 <имя_политики>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики клонирования IPv6-трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для отчистки статистики клонирования IPv6-трафика для указанной политики.

33.3.20 policy clear clone-ipv6 <имя_политики> rule <номер_правила>

Очистка статистики правила политики клонирования IPv6-трафика.

Синтаксис

```
policy clear clone <имя_политики> rule <номер_правила>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики клонирования IPv6-трафика.

номер_правила

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999. Если необходимо очистить статистику для нескольких правил, следует выполнить команду clear для каждого из них в отдельности.

Значение по умолчанию

Отсутствует.

33.3.21 policyclearclone-ipv6 <имя_политики> rule <номер_правила> filter

Очистка статистики для фильтра, связанного с указанным правилом политики клонирования IPv6-трафика.

Синтаксис

```
policy clear clone-ipv6 <имя_политики> rule <номер_правила> filter
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики клонирования IPv6-трафика.

номер_правила

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

Значение по умолчанию

Отсутствует.

33.3.22 policy clear clone-ipv6 <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>

Очистка статистики по указанному правилу фильтра, связанного с указанным правилом политики клонирования IPv6-трафика.

Синтаксис

```
policy clear clone-ipv6 <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики клонирования IPv6-трафика.

номер_правила

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

номер_правила_фильтра

Численный идентификатор правила фильтра. Значение должно лежать в диапазоне от 1 до 9999.

Значение по умолчанию

Отсутствует.

33.3.23 policy show clone-ipv6 <имя_политики>

Вывод сведений и статистики для указанной политики клонирования IPv6-трафика.

Синтаксис

```
policy show clone-ipv6 <имя_политики>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики клонирования IPv6-трафика.

Значение по умолчанию

При использовании без параметров отображается сводка для всех политик клонирования IPv6-трафика.

Указания по использованию

Эта команда используется для отображения сведений о выбранной настроенной политике клонирования IPv6-трафика.

Сведения об интерфейсах, к которым применена указанная политика, не выводятся. Для просмотра сведений о политиках клонирования IPv6-трафика, примененных к конкретному интерфейсу, следует применять команду **show interfaces** для интерфейса.

33.3.24 policy show clone-ipv6 <имя_политики> rule <номер_правила>

Вывод конфигурации правила политики клонирования IPv6-трафика.

Синтаксис

```
policy show clone-ipv6 <имя_политики> rule <номер_правила>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики клонирования IPv6-трафика.

номер_правила

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

Значение по умолчанию

Отсутствует.

33.3.25 policy show clone-ipv6 <имя_политики> rule <номер_правила> filter

Вывод сведений о конфигурации и статистике по указанному правилу политики клонирования IPv6-трафика и фильтру, связанному с ним.

Синтаксис

```
policy show clone-ipv6 <имя_политики> rule <номер_правила> filter [detail]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики клонирования IPv6-трафика.

номер_правила

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

detail

Вывод подробных сведений о конфигурации и статистике.

Значение по умолчанию

Отсутствует.

33.3.26 policy show clone-ipv6 <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>

Вывод статистики по указанному правилу фильтра, связанного с указанным правилом политики клонирования IPv6-трафика.

Синтаксис

```
policy show clone-ipv6 <имя_политики> rule <номер_правила> filter rule <номер_правила_фильтра>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_политики

Имя политики клонирования IPv6-трафика.

номер_правила

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

номер_правила_фильтра

Численный идентификатор правила фильтра. Значение должно лежать в диапазоне от 1 до 9999.

Значение по умолчанию

Отсутствует.

34 Маршрутизация многоадресных передач

34.1 Многоадресные передачи

34.1.1 Понятие многоадресной передачи

При одноадресной передаче сетевой трафик передается в единственную точку назначения. Если сетевой трафик необходимо передать в группу точек назначения, то используется многоадресная передача. Многоадресный трафик может быть принят только членами группы точек назначения, прослушивающими многоадресный трафик, т.е. группой многоадресной передачи. Все остальные узлы игнорируют многоадресный трафик.

Центральным понятием многоадресной передачи по IP является членство в группе. Дейтаграммы многоадресной передачи по IP отправляются группе, и только члены этой группы получают дейтаграммы. Группа определяется одним групповым IP-адресом класса D в диапазоне 224.0.0.0–239.255.255.255 (224.0.0.0/4 в формате CIDR). Адреса класса D из указанного диапазона называются групповыми. Сетевой узел-отправитель отсылает многоадресные дейтаграммы на групповой адрес. Сетевые узлы-получатели, на которых настроена многоадресная передача, при установлении подключения к сети сообщают локальному маршрутизатору о необходимости присоединиться к группе.

В интрасети, где каждый узел поддерживает многоадресную передачу, любой сетевой узел может посылать дейтаграммы многоадресной передачи на любой групповой адрес и любой узел может получать многоадресные дейтаграммы от любого группового адреса независимо от его расположения. Для установки членства сетевых узлов в группе используется протокол IGMP. Для переадресации данных многоадресной передачи маршрутизаторы используют протоколы многоадресной маршрутизации, в частности протокол DVMRP.

На следующем рисунке показана интрасеть с поддержкой многоадресной передачи.

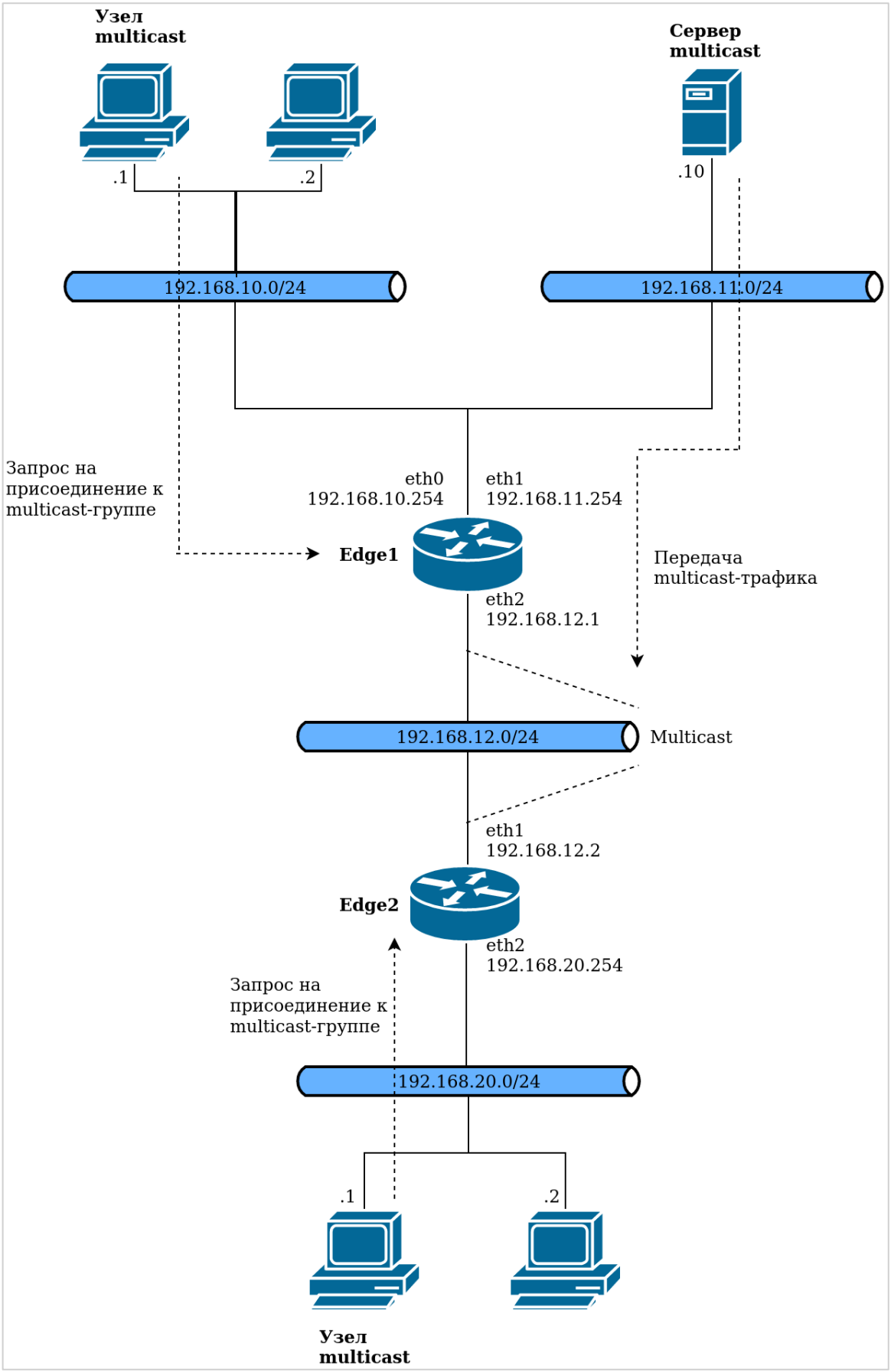


Рисунок 78 – Схема стенда

На данном рисунке сетевые узлы и маршрутизаторы также поддерживают многоадресную передачу, чтобы обеспечить выполнение следующих действий.

- Сетевой узел-отправитель посылает многоадресные дейтаграммы на указанный групповой адрес.
- Маршрутизаторы перенаправляют многоадресные дейтаграммы во все сегменты сети, где имеются члены группы. Маршрутизаторы могут переадресовывать многоадресный трафик по сети, между сетями и по Интернету.
- Сетевые узлы-получатели передают локальному маршрутизатору данные для присоединения к группе и затем получают все дейтаграммы, отправленные на групповой адрес.
- Если сетевой узел-получатель выходит из группы и обнаруживает, что он может оказаться последним членом данной группы в подсети, то он может связаться с локальным маршрутизатором и выйти из группы, сообщив ему о необходимости прекратить переадресацию многоадресных дейтаграмм в данную подсеть.

34.1.2 Преимущества многоадресной передачи IP

Многоадресная передача обеспечивает эффективную поддержку высокоскоростных сетевых приложений для передачи данных с одного адреса на несколько адресов.

- Многоадресная передача может значительно сократить объем сетевого трафика, так как происходит отправка единичной копии данных.
- Узлы можно настроить для многоадресной передачи без обновления оборудования.
- Поскольку современные модели маршрутизаторов поддерживают многоадресную переадресацию и протоколы многоадресной маршрутизации без дополнительной модернизации, использование многоадресной передачи в сети — это практичное и экономичное решение.

Многоадресная передача используется во многих типах приложений для передачи данных с одного адреса на несколько адресов, например следующих.

- Мультимедийные приложения: видеоконференции и коллективные вычисления.
- Автоматическое обнаружение ресурсов в сети.
- Передача данных, например распространение файлов или синхронизация баз данных.
- Поддержка мобильных компьютеров, например обновление удаленной адресной книги.
- Распространение организационных публикаций.

34.2 Протокол DVMRP и его настройка

Маршрутизация многоадресных передач IP в Numa Edge осуществляется службой mrouted с помощью протокола DVMRP (Distance Vector Multicast Routing Protocol), который служит для транспортировки пакетов многоадресных передач IP между сетями. В протоколе DVMRP сочетаются многие возможности протокола RIP и алгоритма урезанного вещания по обратному пути (Truncated Reverse Path Broadcasting, TRPB). Протокол DVMRP является "протоколом внутреннего шлюза"; он предназначен для применения внутри одной автономной системы, но не между различными автономными системами.

Смысл алгоритма TRPB можно кратко сформулировать следующим образом. Во-первых, в качестве маршрута от узла к точке назначения выбирается кратчайший изо всех маршрутов, по которым дейтаграммы из точки назначения пришли в данный узел (алгоритм вещания по обратному пути, или RPB). Во-вторых, вводится понятие группы многоадресной передачи, после чего из дерева передачи для данной группы исключаются поддеревья, не содержащие узлов из этой группы ("обрезка" дерева и буква T в аббревиатуре).

Очень важным отличием DVMRP от RIP является следующее. RIP работает в условиях маршрутизации и передачи дейтаграмм конкретному получателю, в то время как задачей DVMRP является отслеживание путей возврата к отправителю дейтаграмм многоадресных передач.

Пакет DVMRP состоит из небольшого заголовка IGMP фиксированной длины и потока тегированных данных. Элементы потока называются командами.

Для отправки дейтаграмм через шлюзы, не поддерживающие многоадресные передачи, используются туннели. Туннель строится на основе обычных дейтаграмм многоадресных передач в слабой инкапсуляции, в которой используется специальный двухэлементный слабый маршрут IP от отправителя (добавление полного заголовка IP не выполняется). Для передачи информации узлу-отправителю используется сообщение об ошибке ICMP, в данном протоколе служащее для передачи информации не об ошибках.

Алгоритм TRPB передает дейтаграммы многоадресных передач путем вычисления дерева кратчайших (обратных) путей от (физической) сети отправителя до всех возможных получателей дейтаграммы. Каждый

маршрутизатор с поддержкой многоадресных передач должен определить свое место в дереве относительно конкретного отправителя и затем определить, какие из его виртуальных интерфейсов находятся в дереве кратчайших путей. Этот процесс исключения виртуальных интерфейсов, не находящихся в дереве кратчайших путей, называется "отсечением", а исключаемая виртуальная сеть называется "листом".

Листья определяются примерно следующим образом: если какой-нибудь соседний маршрутизатор считает данную виртуальную сеть частью пути до данного получателя, то виртуальная сеть не является листом. В противном случае она является листом. Это функция, определяемая голосованием.

Для предотвращения возникновения циклов и при определении листьев широко используются разделенный горизонт и блокировка бесконечной метрикой.

Маршрутные сообщения DVMRP могут использоваться для трех основных целей: для периодической передачи всей маршрутной информации, для корректной передачи маршрутной информации о недавно изменившихся маршрутах и просто для отправки всех маршрутов в ответ на запрос.

34.2.1 Туннели DVMRP

Протокол DVMRP позволяет настроить маршрутизацию многоадресных передач в туннельном режиме. Это может быть полезно в тех случаях, когда между двумя маршрутизаторами A и B, поддерживающими маршрутизацию многоадресных передач, находится ещё несколько узлов, относительно которых неизвестно, поддерживают ли все они маршрутизацию многоадресных передач. В этом случае можно создать туннель IPIP между A и B и пропустить через него многоадресный трафик, который будет обертываться в обычные одноадресные дейтаграммы IP на узле A и развертываться на узле B (и наоборот). Таким образом, узлы между A и B будут работать с одноадресной дейтаграммой, которую они гарантированно корректно обработают. Кроме того, настройка туннеля может быть полезна в случае, когда подсети X и Y связаны туннелем VPN, через который описанным выше образом может проходить многоадресный трафик.

34.2.2 Настройка протокола DVMRP

Дерево настройки маршрутизации многоадресных передач находится под узлом **protocols dvmrp**. Чтобы включить маршрутизацию многоадресных передач, необходимо ввести следующие команды в режиме настройки:

```
admin@edge# set protocols dvmrp
[edit]
admin@edge# commit
```

В данном случае система Numa Edge запустит службу mrouted, которая будет работать в настройке по умолчанию. Это значит, что маршрутизация многоадресных передач будет осуществляться через все доступные сетевые интерфейсы, поддерживающие многоадресные передачи. Служба mrouted будет отсылать на них запросы DVMRP для поиска в сети других маршрутизаторов с поддержкой многоадресных передач.

ПРИМЕЧАНИЕ Для работы DVMRP multicast маршрутизации требуется минимум 2 работающих multicast интерфейса.

34.2.3 Настройка многоадресных передач на сетевых интерфейсах

Помимо конфигурации по умолчанию, в системе можно установить параметры маршрутизации многоадресных передач на каждый интерфейс, поддерживающий многоадресную передачу.

Выключение маршрутизации многоадресных передач на интерфейсе

Можно явно запретить маршрутизацию многоадресных передач на конкретном интерфейсе. Это может быть полезно в тех случаях, когда машина с установленной маршрутизацией многоадресных передач подключена через некоторый интерфейс к Интернету, а администратору нужно, чтобы трафик многоадресных передач не перенаправлялся и не маршрутизировался на этот интерфейс. Предположим, что это интерфейс eth0. Система позволяет запретить маршрутизацию многоадресных передач на этот интерфейс следующим образом:

```
[edit]
admin@edge# set protocols dvmrp interface eth0 disable
```

Настройка метрики и порога для интерфейса

Для каждого сетевого интерфейса, поддерживающего многоадресную маршрутизацию, можно определить ещё два параметра многоадресной маршрутизации — метрику (metric) и порог (threshold).

Метрика (metric) интерфейса — это своеобразный "вес" или "приоритет" дейтаграмм, отправляемых с интерфейса. Метрика непосредственно влияет на многоадресную маршрутизацию. Чем она ниже, тем выше приоритет дейтаграмм на данном интерфейсе и тем более вероятно, что при маршрутизации будет выбран удалённый маршрут, видимый через интерфейс с наименьшей метрикой. Значение метрики по умолчанию равно 1.

ВНИМАНИЕ Система не обрабатывает маршруты с суммарной метрикой больше 31. Общая рекомендация заключается в том, чтобы метрика была настолько мала, насколько это возможно.

Пример настройки:

```
[edit]
admin@edge# set protocols dvmrp interface eth3 metric 2
```

Порог (threshold) — это минимальное значение времени жизни (TTL) дейтаграммы многоадресной передачи. Порог может быть использован для ограничения "области видимости" принимаемых дейтаграмм. Так, каждый многоадресный маршрутизатор сравнивает значение TTL входящей дейтаграммы с установленным порогом. Если TTL дейтаграммы меньше порога, маршрутизатор не будет пытаться отправить её дальше. В противном случае он уменьшит TTL дейтаграммы на единицу и отправит её на следующую точку маршрута. Значение порога по умолчанию равно 1.

Пример настройки:

```
[edit]
admin@edge# set protocols dvmrp interface eth3 threshold 10
```

34.2.4 Настройка маршрутизации многоадресных передач через туннель

Система позволяет настроить от 1 до 10 туннелей для многоадресной передачи (mtun0 .. mtun9 соответственно). Каждый туннель для многоадресной передачи принимает 2 основных параметра:

- Локальный IP-адрес: IP-адрес на данной машине, с которого будет идти трафик многоадресной передачи, оборачиваемый в одноадресную.
- Удалённый IP-адрес или имя удалённого узла: точка маршрута, на которой многоадресная передача, обернутая в одноадресную, будет разворачиваться обратно в многоадресную.

Например:

```
[edit]
admin@edge# set protocols dvmrp tunnel mtun0 local 192.168.1.77
[edit]
admin@edge# set protocols dvmrp tunnel mtun0 remote 192.168.2.99
```

Или

```
[edit]
admin@edge# set protocols dvmrp tunnel mtun0 local 10.0.0.1
[edit]
admin@edge# set protocols dvmrp tunnel mtun0 remote myhost.mydomain
```

34.2.5 Настройка административно ограниченных областей

Административно ограниченные области, описанные в RFC 2365, дают возможность использовать подсети с многоадресной передачей в диапазоне адресов от 239.0.0.0 до 239.255.255.255 для административных (внутренних) целей, например, для ограничения областей видимости. Предположим, что адреса 239.0.0.1 и

239.1.1.1 используются в локальной сети с многоадресной маршрутизацией для административных (внутренних) целей. Администратору требуется, чтобы дейтаграммы, принадлежащие группам 239.0.0.1 и 239.1.1.1, не маршрутизировались и не перенаправлялись многоадресным маршрутизатором за пределы локальной сети. Чтобы добиться этого, можно поставить ограничения на туннели и интерфейсы.

Прежде всего системе нужно указать, какие именно подсети считаются административно ограниченными:

```
[edit]
admin@edge# set protocols dvmrp alias adress-group-one netmask 239.0.0.0/16
[edit]
admin@edge# set protocols dvmrp alias adress-group-two netmask 239.1.0.0/16
```

Впоследствии псевдонимы adress-group-one и adress-group-two можно использовать для ограничения областей видимости:

```
[edit]
admin@edge# set protocols dvmrp interface eth1 bound adress-group-one
[edit]
admin@edge# set protocols dvmrp interface eth1 bound adress-group-two
[edit]
admin@edge# set protocols dvmrp tunnel mtun0 bound adress-group-two
```

Это значит, что сеть adress-group-one видима только через интерфейс eth1, а сеть adress-group-two видима через интерфейс eth1 и туннель mtun0. Дейтаграммы с адресов adress-group-one и adress-group-two не будут перенаправляться на другие интерфейсы.

34.3 Примеры

34.3.1 Простейший пример настройки протокола DVMRP в сети

В данном разделе приведен простейший пример настройки маршрутизации многоадресных передач.

На приведенном ниже рисунке показана топология сети.

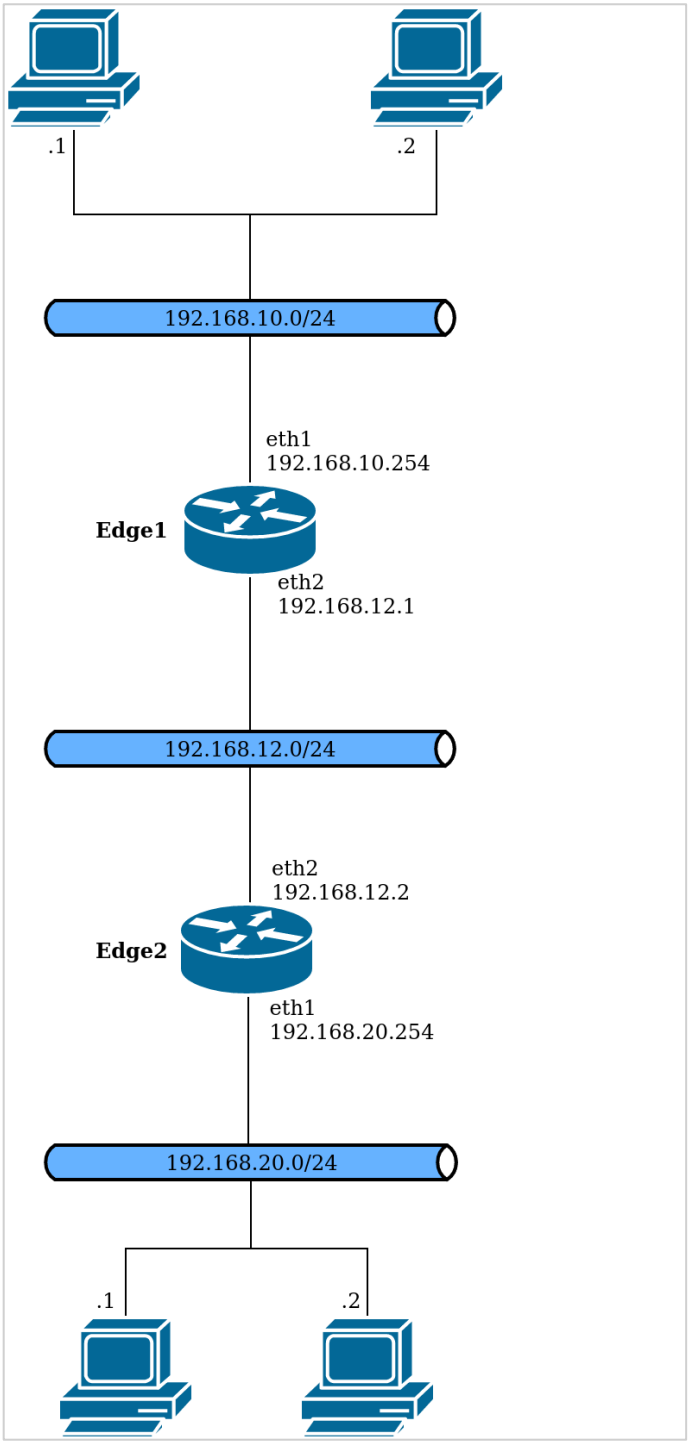


Рисунок 79 – Топология сети

На маршрутизаторах edge1 и edge2 настроен протокол DVMRP. Клиентские компьютеры Client1 и Client2 видят друг друга за счёт статической маршрутизации между маршрутизаторами edge1 и edge2. Ниже представлена последовательность команд для настройки протокола DVMRP в данной сети.

Пример 312 - Простейший пример настройки многоадресной маршрутизации

Действие	**Команда**
IP-адрес на интерфейсе eth1 маршрутизатора edge1.	`[edit]` `admin@edge1# set interfaces ethernet eth1 address 192.168.10.254/24`
IP-адрес на интерфейсе eth2 маршрутизатора edge1.	`[edit]` `admin@edge1# set interfaces ethernet eth2 address 192.168.12.1/24`
Включение поддержки DVMRP на edge1.	`[edit]`

Действие	Команда
	admin@edge1# set protocols dvmrp
Установка порога DVMRP на интерфейсе eth1 на edge1.	[edit] admin@edge1# set protocols dvmrp interface eth1 threshold 5
Установка порога DVMRP на интерфейсе eth2 на edge1.	[edit] admin@edge1# set protocols dvmrp interface eth2 threshold 5
Установка статического маршрута до edge2 для одноадресных передач на edge1.	[edit] admin@edge1# set protocols static route 192.168.20.0/24 next-hop 192.168.12.2
Установка статического маршрута до edge2 для многоадресных передач на edge1.	[edit] admin@edge1# set protocols static route 224.0.0.0/16 next-hop 192.168.12.2
Фиксация изменений.	[edit] admin@edge1# commit

Вывод настройки интерфейсов на edge1.	[edit]
	admin@edge1# show interfaces
	ethernet eth1 {
	address 192.168.10.254/24
	}
	ethernet eth2 {
	address 192.168.12.1/24
	}

Вывод настройки протоколов на edge1.	[edit]
	admin@edge1# show protocols
	dvmrp {
	interface eth1 {
	threshold 5
	}
	interface eth2 {
	threshold 5
	}
	}
	static {
	route 192.168.20.0/24 {
	next-hop 192.168.12.2 {
	}
	}
	route 224.0.0.0/16 {
	next-hop 192.168.12.2 {
	}
	}
	}

IP-адрес на интерфейсе eth1 маршрутизатора edge2.	[edit] admin@edge2# set interfaces ethernet eth1 address 192.168.20.254/24
IP-адрес на интерфейсе eth2 маршрутизатора edge2.	[edit] admin@edge2# set interfaces ethernet eth2 address 192.168.12.2/24
Включение поддержки DVMRP на edge2.	[edit] admin@edge2# set protocols dvmrp
Установка порога DVMRP на интерфейсе eth1 на edge2.	[edit] admin@edge2# set protocols dvmrp interface eth1 threshold 5
Установка порога DVMRP на интерфейсе eth2 на edge2.	[edit] admin@edge2# set protocols dvmrp interface eth2 threshold 5
Установка статического маршрута до edge1 для одноадресных передач на edge2.	[edit] admin@edge2# set protocols static route

Действие	Команда
	`192.168.10.0/24 next-hop 192.168.12.1`
Установка статического маршрута до edge1 для многоадресных передач на edge2.	`[edit]` `admin@edge2# set protocols static route 224.0.0.0/16 next-hop 192.168.12.1`
Фиксация изменений.	`[edit]` `admin@edge2# commit`

Вывод настройки интерфейсов на edge2.	`[edit]`
	`admin@edge2# show interfaces`
	`ethernet eth1 {`
	`address 192.168.20.254/24`
	`}`
	`ethernet eth2 {`
	`address 192.168.12.2/24`
	`}`

Вывод настройки протоколов на edge2.	`admin@edge2# show protocols`
	`dvmrp {`
	`interface eth1 {`
	`threshold 5`
	`}`
	`interface eth2 {`
	`threshold 5`
	`}`
	`}`
	`static {`
	`route 192.168.10.0/24 {`
	`next-hop 192.168.12.1 {`
	`}`
	`}`
	`route 224.0.0.0/16 {`
	`next-hop 192.168.12.1 {`
	`}`
	`}`
	`}`

34.3.2 Пример настройки протокола DVMRP с использованием туннелей

В данном разделе приведен более сложный пример настройки протокола DVMRP. Настраивается туннель DVMRP, по которому многоадресная передача проходит через маршрутизатор, вообще не поддерживающий многоадресные передачи.

Как было описано выше, система в туннельном режиме может оборачивать пакеты многоадресной передачи в пакеты одноадресной передачи, которые в свою очередь передаются через туннель. Топология сети приведена на следующем рисунке:

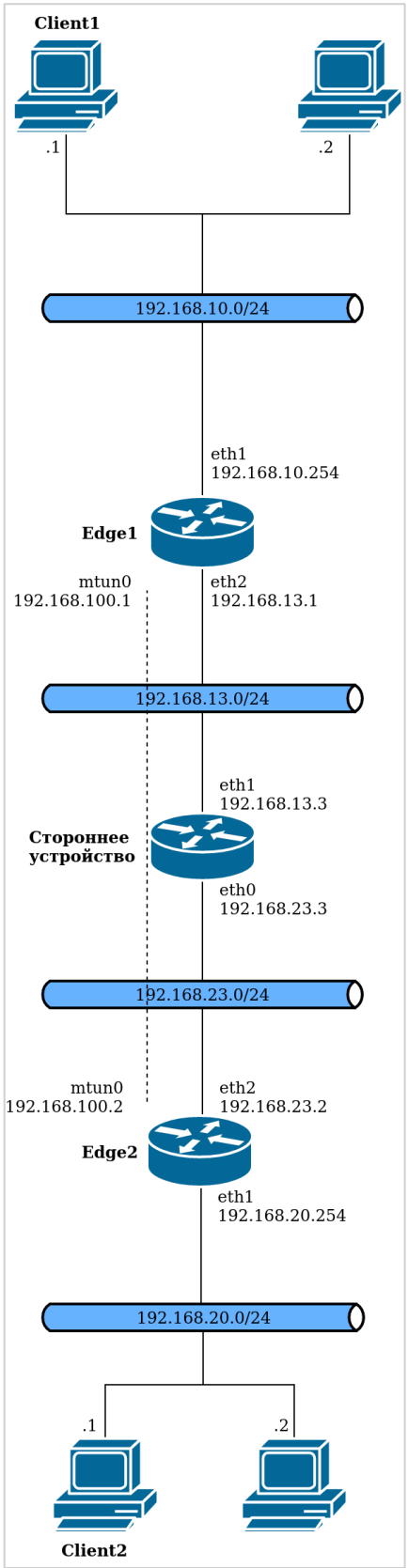


Рисунок 80 – Схема стенда

В примере описана ситуация, когда 2 маршрутизатора (edge1 и edge2) связаны туннелем DVMRP через промежуточный маршрутизатор (Стороннее устройство), который не поддерживает многоадресную передачу.

- Шлюз по умолчанию на edge1: 192.168.13.3.
- Шлюз по умолчанию на edge2: 192.168.23.3.
- Устройства в локальной сети edge1 имееют шлюз по умолчанию 192.168.10.254.

- Устройства в локальной сети edge2 имееют шлюз по умолчанию 192.168.20.254.
- На стороннем устройстве, через которое связаны edge1 и edge2, многоадресная передача не поддерживается.

Порядок выполнения команд, данный в примере, существенен: к моменту настройки туннеля его удаленный конец должен быть достижим.

Пример 313 - Пример настройки протокола DVMRP с использованием туннелей

Действие	**Команда**
IP-адрес на интерфейсе eth1 маршрутизатора edge1.	`[edit]` `admin@edge1# set interfaces ethernet eth1 address 192.168.10.254/24`
IP-адрес на интерфейсе eth2 маршрутизатора edge1.	`[edit]` `admin@edge1# set interfaces ethernet eth2 address 192.168.13.1/24`
Включение поддержки DVMRP на edge1.	`[edit]` `admin@edge1# set protocols dvmrp`
Установка порога DVMRP на интерфейсе eth3 на edge1.	`[edit]` `admin@edge1# set protocols dvmrp interface eth1 threshold 5`
Установка порога DVMRP на интерфейсе eth4 на edge1.	`[edit]` `admin@edge1# set protocols dvmrp interface eth2 threshold 5`
Фиксация изменений.	`[edit]` `admin@edge1# commit`
IP-адрес на интерфейсе eth1 маршрутизатора edge2	`[edit]` `admin@edge2# set interfaces ethernet eth1 address 192.168.20.254/24`
IP-адрес на интерфейсе eth2 маршрутизатора edge2.	`[edit]` `admin@edge2# set interfaces ethernet eth2 address 192.168.23.2/24`
Включение поддержки DVMRP на edge2.	`[edit]` `admin@edge2# set protocols dvmrp`
Установка порога DVMRP на интерфейсе eth3 на edge2.	`[edit]` `admin@edge2# set protocols dvmrp interface eth1 threshold 5`
Установка порога DVMRP на интерфейсе eth2 на edge2.	`[edit]` `admin@edge2# set protocols dvmrp interface eth2 threshold 5`
Фиксация изменений.	`[edit]` `admin@edge2# commit`
Включение туннеля DVMRP на edge1.	`[edit]` `admin@edge1# set protocols dvmrp tunnel mtun0`
Установка локального конца туннеля DVMRP на edge1.	`[edit]` `admin@edge1# set protocols dvmrp tunnel mtun0 local 192.168.100.1`
Установка удаленного конца туннеля DVMRP на edge1.	`[edit]` `admin@edge1# set protocols dvmrp tunnel mtun0 remote 192.168.100.2`
Установка порога DVMRP по умолчанию для туннеля на edge1.	`[edit]` `admin@edge1# set protocols dvmrp tunnel mtun0 threshold 5`
Установка статического маршрута до стороннего устройства на edge1.	`[edit]` `admin@edge1# set protocols static route 0.0.0.0/0 next-hop 192.168.13.3`
Установка статического маршрута до локальной сети edge2 на edge1.	`[edit]` `admin@edge1# set protocols static route`

Действие	Команда
	`192.168.20.0/24 next-hop 192.168.100.2`
Фиксация изменений.	`[edit]` `admin@edge1# commit`
Включение туннеля DVMRP на edge2.	`[edit]` `admin@edge2# set protocols dvmrp tunnel mtun0`
Установка локального конца туннеля DVMRP на edge2.	`[edit]` `admin@edge2# set protocols dvmrp tunnel mtun0 local 192.168.100.2`
Установка удаленного конца туннеля DVMRP на edge2.	`[edit]` `admin@edge2# set protocols dvmrp tunnel mtun0 remote 192.168.100.1`
Установка порога DVMRP по умолчанию для туннеля на edge2.	`[edit]` `admin@edge2# set protocols dvmrp tunnel mtun0 threshold 5`
Установка статического маршрута до стороннего устройства на edge2.	`[edit]` `admin@edge2# set protocols static route 0.0.0.0/0 next-hop 192.168.23.3`
Установка статического маршрута до локальной сети edge1 на edge2.	`[edit]` `admin@edge1# set protocols static route 192.168.10.0/24 next-hop 192.168.100.1`
Фиксация изменений.	`[edit]` `admin@edge2# commit`

Вывод настройки интерфейсов на edge1.	`[edit]`
	`admin@edge1# show interfaces`
	`ethernet eth1 {`
	`address 192.168.10.254/24`
	`}`
	`ethernet eth2 {`
	`address 192.168.13.1/24`
	`}`

Вывод настройки протоколов на edge1.	`[edit]`
	`admin@edge1# show protocols`
	`dvmrp {`
	`interface eth1 {`
	`threshold 5`
	`}`
	`interface eth2 {`
	`threshold 5`
	`}`
	`tunnel mtun0 {`
	`local 192.168.100.1`
	`remote 192.168.100.2`
	`}`
	`}`
	`static {`
	`route 0.0.0.0/0 {`
	`next-hop 192.168.13.3 {`
	`}`
	`}`
	`route 192.168.20.0/24 {`
	`next-hop 192.168.100.2 {`
	`}`
	`}`
	`}`

Вывод настройки интерфейсов на edge2.	`[edit]`
	`admin@edge2# show interfaces`
	`ethernet eth1 {`
	`address 192.168.20.254/24`

Действие	Команда

	}
	ethernet eth2 {
	address 192.168.23.2/24
	}

Вывод настройки протоколов на edge2.	[edit]
	admin@edge2# show protocols
	dvmrp {
	interface eth1 {
	threshold 5
	}
	interface eth2 {
	threshold 5
	}
	tunnel mtun0 {
	local 192.168.100.2
	remote 192.168.100.1
	}
	}
	static {
	route 0.0.0.0/0 {
	next-hop 192.168.23.3 {
	}
	}
	route 192.168.10.0/24 {
	next-hop 192.168.100.1 {
	}
	}
	}

Клиенты client1 и client2 (это, например, обычные компьютеры под управлением любой ОС, поддерживающей многоадресные передачи) должны быть настроены в соответствии с топологией сети, представленной выше. Так, чтобы client1 видел client2, например:

- client1: IP-адрес 192.168.10.1/24, шлюз по умолчанию 192.168.10.254
- client2: IP-адрес 192.168.20.1/24, шлюз по умолчанию 192.168.20.254

34.4 Команды маршрутизации многоадресных передач

Команды настройки	
protocols dvmrp	Включение протокола DVMRP и службы маршрутизации многоадресных передач в системе.
protocols dvmrp alias <псевдоним> netmask <подсеть_IPV4>	Определение административно ограниченной подсети с многоадресной передачей.
protocols dvmrp interface <интерфейс>	Включение протокола DVMRP на интерфейсе.
protocols dvmrp interface <интерфейс> bound <псевдоним>	Связывание интерфейса с административно ограниченной подсетью для многоадресной передачи.
protocols dvmrp interface <интерфейс> disable	Отключение протокола DVMRP на интерфейсе без удаления настройки протокола.
protocols dvmrp interface <интерфейс> metric <метрика>	Назначение метрики DVMRP для интерфейса.
protocols dvmrp interface <интерфейс> threshold <порог>	Назначение порога (минимального времени жизни дейтаграмм) на интерфейсе.
protocols dvmrp tunnel <имя_туннеля>	Определение туннеля DVMRP.
protocols dvmrp tunnel <имя_туннеля> bound <псевдоним>	Связывание туннеля DVMRP с административно ограниченной подсетью.
protocols dvmrp tunnel <имя_туннеля> local <локальный_узел>	Указание локального IP-адреса туннеля DVMRP.

protocols dvmrp tunnel <имя_туннеля> metric <метрика>	Установка метрики для туннеля DVMRP.
protocols dvmrp tunnel <имя_туннеля> remote <удалённый_узел>	Установка IP-адреса удаленного конца туннеля DVMRP.
protocols dvmrp tunnel <имя_туннеля> threshold <порог>	Установка порога (минимального времени жизни дейтаграмм) для туннеля DVMRP.
Эксплуатационные команды	
show ip dvmrp	Отображение статистики и таблиц маршрутизации протокола DVMRP.

34.4.1 protocols dvmrp

Включение протокола DVMRP и службы маршрутизации многоадресных передач в системе.

Синтаксис

```
set protocols dvmrp
delete protocolsd dvmrp
show protocols dvmrp
```

Режим интерфейса

Режим настройки

Ветвь конфигурации

```
protocols {
    dvmrp {
    }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда служит для управления протоколом DVMRP и службой mrouted на машрутизаторе.

Форма **set** этой команды служит для включения протокола DVMRP и запуска службы mrouted на маршрутизаторе.

ПРИМЕЧАНИЕ Для удачной фиксации настройки необходимо наличие на маршрутизаторе как минимум двух полностью настроенных интерфейсов, на которых включен протокол DVMRP.

Форма **delete** этой команды служит для отключения протокола DVMRP и остановки службы mrouted на маршрутизаторе.

Форма **show** этой команды служит для отображения настройки протокола DVMRP на маршрутизаторе.

34.4.2 protocols dvmrp alias <псевдоним> netmask <подсеть_IPV4>

Определение административно ограниченной подсети с многоадресной передачей.

Синтаксис

```
set protocols dvmrp alias <псевдоним> [netmask <подсеть_ipv4>]
delete protocols dvmrp alias <псевдоним> [netmask]
show protocols dvmrp alias <псевдоним> [netmask]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    dvmrp {
        alias псевдоним {
            netmask подсеть_ipv4
        }
    }
}
```

Параметры

псевдоним

Имя административно ограниченной подсети с многоадресной передачей.

подсеть_ipv4

Подсеть, с которой связывается псевдоним. В соответствии с RFC 2365, подсеть должна находиться в пределах 239.0.0.0/8.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для управления административно ограниченными подсетями в соответствии с RFC 2365.

Форма **set** этой команды используется для определения административно ограниченной подсети. Сетевая маска, если она указывается, должна определять подсеть в области от 239.0.0.0 до 239.255.255.255.

Форма **delete** этой команды используется для удаления административно ограниченной подсети, ее псевдонима или всех административно ограниченных подсетей (в зависимости от варианта формата команды).

Форма **show** этой команды используется для отображения настройки административно ограниченных подсетей.

34.4.3 protocols dvmrp interface <интерфейс>

Включение протокола DVMRP на интерфейсе.

Синтаксис

```
set protocols dvmrp interface <интерфейс>
delete protocols dvmrp interface <интерфейс>
show protocols dvmrp interface <интерфейс>
```

Режим интерфейса

Режим настройки

Ветвь конфигурации

```
protocols {
    dvmrp {
        interface интерфейс
    }
}
```

Параметры

интерфейс

Интерфейс, на котором включается протокол DVMRP.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для включения протокола DVMRP на интерфейсе системы.

Форма **set** этой команды используется для включения протокола DVMRP на интерфейсе системы.

Форма **delete** этой команды используется для постоянного отключения протокола DVMRP на интерфейсе системы и удаления узла конфигурации protocols dvmrp interface.

Форма **show** этой команды используется для отображения настройки протокола DVMRP на указанном интерфейсе.

34.4.4 protocols dvmrp interface <интерфейс> bound <псевдоним>

Связывание интерфейса с административно ограниченной подсетью для многоадресной передачи.

Синтаксис

```
set protocols dvmrp interface <интерфейс> bound <псевдоним>
delete protocols dvmrp interface <интерфейс> bound <псевдоним>
show protocols dvmrp interface <интерфейс> bound
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    dvmrp {
        interface интерфейс {
            bound псевдоним
        }
    }
}
```

Параметры

интерфейс

Имя интерфейса, с которым связывается административно ограниченная подсеть.

псевдоним

Имя связываемой административно ограниченной подсети.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для управления связыванием интерфейса с административно ограниченными подсетями. Интерфейс может быть связан с несколькими административно ограниченными подсетями; административно ограниченная подсеть может быть связана с несколькими интерфейсами.

Форма **set** этой команды используется для связывания интерфейса с административно ограниченной подсетью.

Форма **delete** этой команды используется для удаления связывания интерфейса с указанной административно ограниченной подсетью или (если подсеть не указана) со всеми административно ограниченными подсетями.

Форма **show** этой команды предназначена для отображения настройки связывания интерфейса с административно ограниченными подсетями.

34.4.5 protocols dvmrp interface <интерфейс> disable

Отключение протокола DVMRP на интерфейсе без удаления настройки протокола.

Синтаксис

```
set protocols dvmrp interface <интерфейс> disable
delete protocols dvmrp interface <интерфейс> disable
show protocols dvmrp interface <интерфейс> disable
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    dvmrp {
        interface интерфейс {
            disable
        }
    }
}
```

Параметры

интерфейс

Идентификатор интерфейса, на котором отключается настроенный протокол DVMRP.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для временного отключения протокола DVMRP на указанном интерфейсе без удаления настройки протокола и тем самым предотвращения маршрутизации многоадресных передач через указанный интерфейс.

Форма **set** данной команды используется для отключения протокола DVMRP на указанном интерфейсе.

Форма **delete** данной команды используется для отмены режима отключения протокола DVMRP и разрешения тем самым маршрутизации многоадресных передач через этот интерфейс.

Форма **show** данной команды используется для просмотра состояния отключения протокола DVMRP на указанном интерфейсе.

34.4.6 protocols dvmrp interface <интерфейс> metric <метрика>

Назначение метрики DVMRP для интерфейса.

Синтаксис

```
set protocols dvmrp interface <интерфейс> metric <метрика>
delete protocols dvmrp interface <интерфейс> metric
show protocols dvmrp interface <интерфейс> metric
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    dvmrp {
        interface интерфейс {
```

```
            metric метрика
        }
    }
}
```

Параметры

интерфейс

Идентификатор интерфейса, на котором отключается настроенный протокол DVMRP.

метрика

Числовое значение метрики, назначаемой интерфейсу. Значение должно находиться в диапазоне от 1 до 10.

Значение по умолчанию

Интерфейсу назначается метрика, равная 1.

Указания по использованию

Данная команда используется для назначения метрики интерфейсу, участвующему в маршрутизации многоадресных передач. Рекомендуется указывать как можно меньшие значения метрики.

ВНИМАНИЕ Маршрутизатор многоадресного трафика не может обрабатывать маршруты, сумма метрик которых превышает 31.

Форма **set** этой команды используется для назначения метрики указанному интерфейсу.

Форма **delete** этой команды используется для удаления ранее назначенного значения метрики и сброса его в значение по умолчанию.

Форма **show** этой команды используется для отображения настройки метрики на интерфейсе.

34.4.7 protocols dvmrp interface <интерфейс> threshold <порог>

Назначение порога (минимального времени жизни дейтаграмм) на интерфейсе.

Синтаксис

```
set protocols dvmrp interface <интерфейс> threshold <порог>
delete protocols dvmrp interface <интерфейс> threshold
show set protocols dvmrp interface <интерфейс> threshold
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    dvmrp {
        interface <интерфейс> {
            threshold <порог>
        }
    }
}
```

Параметры

интерфейс

Интерфейс, на котором назначается метрика.

порог

Числовое значение порога, назначаемого интерфейсу. Значение должно лежать в диапазоне 1-255.

Значение по умолчанию

Интерфейсу назначается порог, равный 1.

Указания по использованию

Данная команда используется для назначения порога интерфейсу, участвующему в маршрутизации многоадресных передач. Дейтаграмма со значением времени жизни (TTL), меньшем порога, отбрасывается. Если у дейтаграммы значение TTL больше или равно порогу, из TTL вычитается единица, и дейтаграмма передаётся на следующий узел.

Форма **set** этой команды используется для назначения порога указанному интерфейсу.

Форма **delete** этой команды используется для удаления ранее назначенного значения порога и сброса его в значение по умолчанию.

Форма **show** этой команды используется для отображения настройки порога на интерфейсе.

34.4.8 protocols dvmrp tunnel <имя_туннеля>

Определение туннеля DVMRP.

Синтаксис

```
set protocols dvmrp tunnel <имя_туннеля>
delete protocols dvmrp tunnel <имя_туннеля>
show protocols dvmrp tunnel
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    dvmrp {
        tunnel имя_туннеля
    }
}
```

Параметры

имя_туннеля

Имя туннеля DVMRP. Допустимы значения mtun0-mtun9.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для создания туннеля DVMRP.

Форма **set** этой команды используется для создания туннеля DVMRP с указанными именем.

Форма **delete** этой команды используется для удаления туннеля DVMRP с указанным именем.

Форма **show** этой команды используется для отображения настроенных туннелей DVMRP и всех их параметров.

34.4.9 protocols dvmrp tunnel <имя_туннеля> bound <псевдоним>

Связывание туннеля DVMRP с административно ограниченной подсетью.

Синтаксис

```
set protocols dvmrp tunnel <имя_туннеля> bound <псевдоним>
delete protocols dvmrp tunnel <имя_туннеля> bound  <псевдоним>
```

```
show protocols dvmrp tunnel <имя_туннеля> bound
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    dvmrp {
        tunnel имя_туннеля {
            bound псевдоним
        }
    }
}
```

Параметры

имя_туннеля

Имя туннеля DVMRP. Допустимы значения mtun0-mtun9.

псевдоним

Псевдоним административно ограниченной подсети, связываемой с туннелем DVMRP.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для связывания административно ограниченной подсети с туннелем DVMRP для пропускания многоадресной передачи через туннель.

Форма **set** этой команды используется для связывания административно ограниченной подсети с туннелем DVMRP. Допускается связывание более чем с одной административно ограниченной подсетью.

Форма **delete** этой команды используется для удаления связывания административно ограниченной подсети (если она указана явно) или всех всех административно ограниченных подсетей, связанных с туннелем DVMRP.

Форма **show** этой команды используется для отображения настройки связывания туннеля с административно ограниченными подсетями.

34.4.10 protocols dvmrp tunnel <имя_туннеля> local <локальный_узел>

Указание локального IP-адреса туннеля DVMRP.

Синтаксис

```
set protocols dvmrp tunnel <имя_туннеля> local <локальный_узел>
delete protocols dvmrp tunnel <имя_туннеля> local
show protocols dvmrp tunnel <имя_туннеля> local
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    dvmrp {
        tunnel имя_туннеля {
            local локальный_IP-адрес_туннеля
        }
    }
```

```
}
```

Параметры

имя_туннеля

Имя туннеля DVMRP. Допустимы значения mtun0-mtun9.

локальный_узел

IPv4-адрес локального конца туннеля DVMRP. Этот адрес должен быть настроен на одном из интерфейсов системы.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для установки IP-адреса локального конца туннеля DVMRP.

Форма **set** этой команды используется для установки IP -адреса локального конца туннеля DVMRP. Для успешной фиксации настройки должны быть установлены адреса как локального, так и удаленного концов туннеля.

Форма **delete** этой команды служит для удаления настроенного IP-адреса локального конца туннеля. При фиксации настройки после выдачи формы delete данной команды настроенный ранее туннель будет удален.

Форма **show** этой команды используется для отображения настроенного IP-адреса локального конца туннеля.

34.4.11 protocols dvmrp tunnel <имя_туннеля> metric <метрика>

Установка метрики для туннеля DVMRP.

Синтаксис

```
set protocols dvmrp tunnel <имя_туннеля> metric <метрика>
delete protocols dvmrp tunnel <имя_туннеля> metric
show protocols dvmrp tunnel <имя_туннеля> metric
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    dvmrp {
        tunnel имя_туннеля {
            metric метрика
        }
    }
}
```

Параметры

имя_туннеля

Имя туннеля DVMRP. Допустимы значения mtun0-mtun9.

метрика

Числовое значение метрики, назначаемой туннелю. Значение должно находиться в диапазоне от 1 до 10.

Значение по умолчанию

Туннелю назначается метрика, равная 1.

Указания по использованию

Данная команда используется для назначения метрики туннелю DVMRP. Рекомендуется указывать как можно меньшие значения метрики.

ВНИМАНИЕ Маршрутизатор многоадресного трафика не может обрабатывать маршруты, сумма метрик которых превышает 31.

Форма **set** этой команды используется для назначения метрики указанному туннелю.

Форма **delete** этой команды используется для удаления ранее назначенного значения метрики и сброса его в значение по умолчанию.

Форма **show** этой команды используется для отображения настройки метрики для туннеля.

34.4.12 protocols dvmrp tunnel <имя_туннеля> remote <удалённый_узел>

Установка IP-адреса удаленного конца туннеля DVMRP.

Синтаксис

```
set protocols dvmrp tunnel <имя_туннеля> remote <удаленный_узел>
delete protocols dvmrp tunnel <имя_туннеля> remote
show protocols dvmrp tunnel <имя_туннеля> remote
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
    dvmrp {
        tunnel имя_туннеля {
            remote удаленный_узел
        }
    }
}
```

Параметры

имя_туннеля

Имя туннеля DVMRP. Допустимы значения mtun0-mtun9.

удаленный_узел

Параметр для подключения к удаленному концу туннеля DVMRP. Может быть задан в виде IP-адреса или имени узла.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для установки IP-адреса или имени узла удаленного конца туннеля DVMRP.

Форма **set** этой команды используется для установки IP -адреса или имени узла удаленного конца туннеля DVMRP. Для успешной фиксации настройки должны быть установлены адреса как локального, так и удаленного концов туннеля.

Форма **delete** этой команды служит для удаления настроенного IP-адреса удаленного конца туннеля. При фиксации настройки после выдачи формы delete данной команды настроенный ранее туннель будет удален.

Форма **show** этой команды используется для отображения настроенного IP-адреса удаленного конца туннеля.

34.4.13 protocols dvmrp tunnel <имя_туннеля> threshold <порог>

Установка порога (минимального времени жизни дейтаграмм) для туннеля DVMRP.

Синтаксис

```
set protocols dvmrp tunnel <имя_туннеля> threshold <порог>
delete protocols dvmrp tunnel <имя_туннеля> threshold
show protocols dvmrp tunnel <имя_туннеля> threshold
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
protocols {
   dvmrp {
      tunnel имя_туннеля {
         threshold порог
      }
   }
}
```

Параметры

имя_туннеля

Имя туннеля DVMRP. Допустимы значения mtun0-mtun9.

порог

Числовое значение порога, назначаемого туннелю. Значение должно лежать в диапазоне 1-255.

Значение по умолчанию

Туннелю назначается порог, равный 1.

Указания по использованию

Данная команда используется для назначения порога туннелю DVMRP. Дейтаграмма со значением времени жизни (TTL), меньшем порога, отбрасывается. Если у дейтаграммы значение TTL больше или равно порогу, из TTL вычитается единица, и дейтаграмма передаётся на следующий узел.

Форма **set** этой команды используется для назначения порога указанному туннелю.

Форма **delete** этой команды используется для удаления ранее назначенного значения порога и сброса его в значение по умолчанию.

Форма **show** этой команды используется для отображения настройки порога на туннеле.

34.4.14 show ip dvmrp

Отображение статистики и таблиц маршрутизации протокола DVMRP.

Синтаксис

```
show ip dvmrp
```

Режим интерфейса

Эксплуатационный режим

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует

Указания по использованию

Команда используется для отображения статистики и таблиц маршрутизации протокола DVMRP на данном маршрутизаторе.

35 DHCP

35.1 Обзор DHCP

Протокол динамической настройки узла (Dynamic Host Configuration Protocol, DHCP) делает возможным динамическое назначение IP-адресов и других сведений о настройке клиентам DHCP. Это позволяет сократить издержки и трудозатраты на настройку и управление сетью. С другой стороны, сервис также создаёт дополнительную нагрузку на сеть и требует некоторого обслуживания.

При использовании DHCP, сервер назначает IP-адрес и другие параметры настройки клиенту на ограниченный промежуток времени. Этот промежуток времени называется *арендой*. Аренда действительна в течение промежутка времени, настраиваемого администратором в системе Numa Edge, или до явного освобождения клиентом адреса.

Для использования службы DHCP администратор определяет пул IP-адресов в каждой подсети, управляемой сервером DHCP. Каждый пул адресов DHCP сопоставляется с подсетью, связанной с системой. Для каждого пула адресов можно указать интервал времени, в течение которого адрес будет допустимым (длительность аренды). Длительность аренды по умолчанию равна 24 часам. Кроме того, можно указать несколько различных серверов (например, DNS, WINS, SMTP, ...), доступных клиенту в подсети.

Также есть возможность статически сопоставить IP-адрес с MAC-адресом устройства. Служба DHCP осуществляет прослушивание запросов от клиентов DHCP на порту 67 UDP. Пакет запроса позволяет системе определить, на каком интерфейсе расположен клиент. Затем она назначает IP-адрес из подходящего пула и привязывает его к клиенту.

Помимо предоставления сервера DHCP, отдельные интерфейсы системы EDGE можно настроить в качестве клиентов DHCP. Более подробные сведения о клиентских настройках представлены в разделах документации Numa edge по настройке интерфейсов, которые требуется настроить в качестве клиентов DHCP.

В поставляемом Numa Edge по умолчанию включён сервер DHCP для обслуживания управляющего интерфейса. Сервер настроен на раздачу адресов из диапазона 192.168.200.10 — 192.168.200.200 со временем аренды в 24 часа.

35.2 Настройка DHCP

В разделе приводятся следующие примеры:

- настройка пулов адресов DHCP;
- резервирование адресов;
- установка дополнительных параметров настройки DHCP.

35.2.1 Настройка пулов адресов DHCP

При необходимости настройки системы в качестве сервера DHCP для сети, следует настроить пулы адресов DHCP.

В примере выполняется создание трех пулов адресов:

- 192.168.11.100-192.168.11.200. Этот пул адресов обслуживает подсеть 192.168.11.0/24, подключенную к интерфейсу eth1. Для времени аренды оставлено значение по умолчанию 24 часа (86400 секунд). В том пуле адресов будет использоваться сервер имен DNS по адресу 192.168.11.254.
- 192.168.12.100-192.168.12.200. Этот пул адресов обслуживает подсеть 192.168.12.0/24, подключенную к интерфейсу eth2. Для времени аренды оставлено значение по умолчанию 24 часа (86400 секунд). В этом пуле адресов будет использоваться сервер имен DNS по адресу 192.168.12.254.
- 192.168.13.100-192.168.13.200. Этот пул адресов обслуживает подсеть 192.168.13.0/24, подключенную к интерфейсу eth3. Для времени аренды оставлено значение по умолчанию 24 часа (86400 секунд).Для этого пула адресов будет использоваться сервер имен DNS с адресом 192.168.13.254.

На рисунке ниже показан пример настройки пулов адресов.

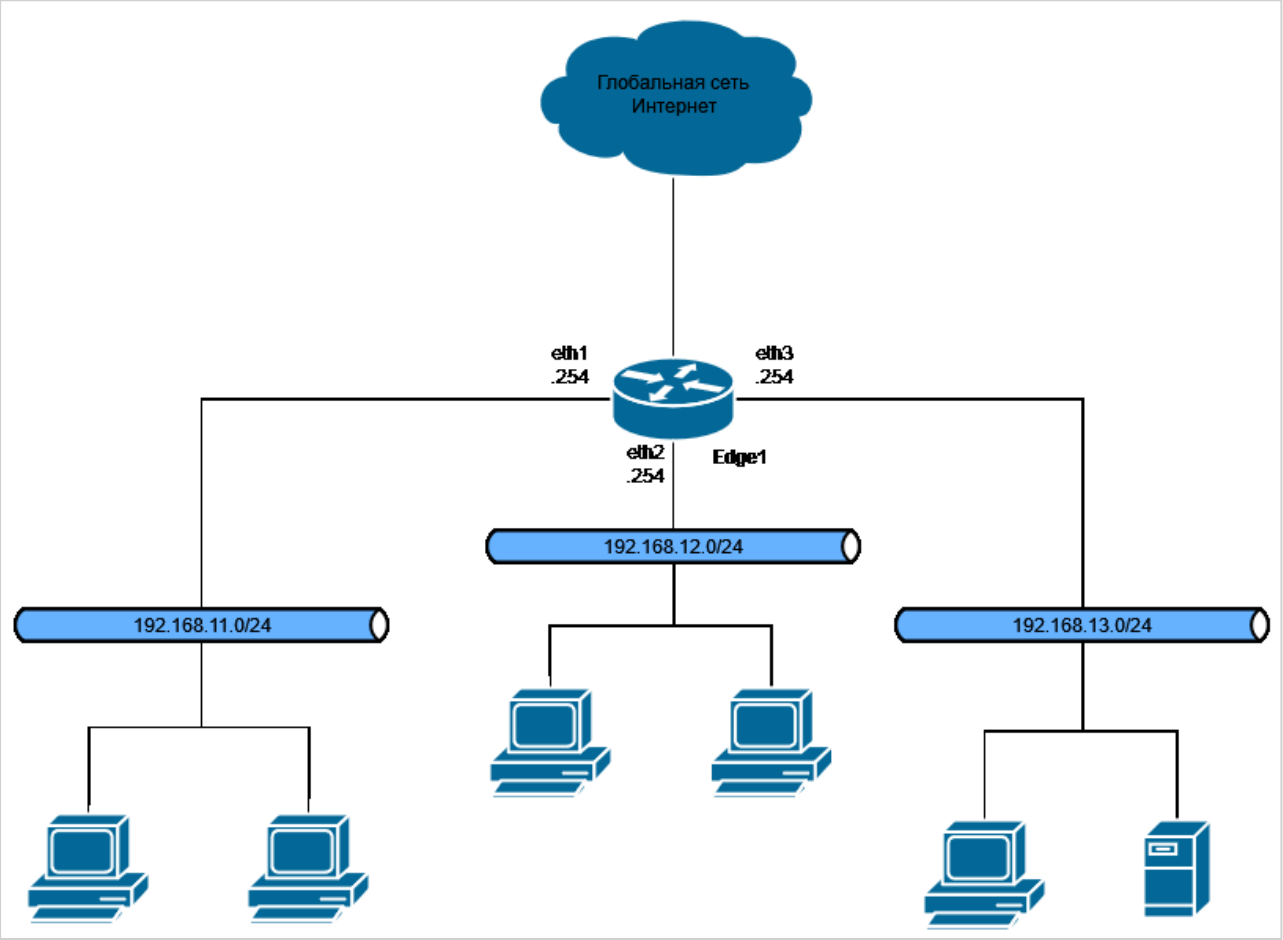


Рисунок 81 – Схема стенда

Для настройки пулов адресов DHCP выполните следующие действия в режиме настройки:

Пример 314 - Настройка пулов адресов DHCP

Действие	**Команда**
Создание узла конфигурации для подсети 192.168.11.0/24. Ввод начального и конечного IP-адресов для пула.	`[edit]` `admin@edge# set service dhcp-server subnet 192.168.11.0/24 start 192.168.11.100 stop 192.168.11.200`
Ввод маршрутизатора по умолчанию для клиентов подсети 192.168.11.0/24.	`[edit]` `admin@edge# set service dhcp-server subnet 192.168.11.0/24 default-router 192.168.11.254`
Ввод сервера DNS для клиентов подсети 192.168.11.0/24.	`[edit]` `admin@edge# set service dhcp-server subnet 192.168.11.0/24 dns-server 192.168.11.254`
Создание узла конфигурации для подсети 192.168.12.0/24. Ввод начального и конечного IP-адресов для пула.	`[edit]` `admin@edge# set service dhcp-server subnet 192.168.12.0/24 start 192.168.12.100 stop 192.168.12.200`
Ввод маршрутизатора по умолчанию для клиентов подсети 192.168.12.0/24.	`[edit]` `admin@edge# set service dhcp-server subnet 192.168.12.0/24 default-router 192.168.12.254`
Ввод сервера DNS для клиентов подсети 192.168.12.0/24.	`[edit]` `admin@edge# set service dhcp-server subnet 192.168.12.0/24 dns-server 192.168.12.254`
Создание узла конфигурации для подсети 192.168.13.0/24. Ввод начального и конечного IP-	`[edit]` `admin@edge# set service dhcp-server subnet`

Действие	Команда
адресов для пула.	`192.168.13.0/24 start 192.168.13.100 stop 192.168.13.200`
Ввод маршрутизатора по умолчанию клиентов подсети 192.168.13.0/24.	`[edit]` `admin@edge# set service dhcp-server subnet 192.168.13.0/24 default-router 192.168.13.254`
Ввод сервера DNS для клиентов подсети 192.168.13.0/24.	`[edit]` `admin@edge# set service dhcp-server subnet 192.168.13.0/24 dns-server 192.168.13.254`
Фиксация изменений.	`[edit]` `admin@edge# commit`

Вывод настройки.	`[edit]`
	`admin@edge# show service dhcp-server`
	`  subnet 192.168.11.0/24 {`
	`  default-router 192.168.11.254`
	`  dns-server 192.168.11.254`
	`  start 192.168.11.100 {`
	`  stop 192.168.11.200`
	`  }`
	`  }`
	`  subnet 192.168.12.0/24 {`
	`  default-router 192.168.12.254`
	`  dns-server 192.168.12.254`
	`  start 192.168.12.100 {`
	`  stop 192.168.12.200`
	`  }`
	`  }`
	`  subnet 192.168.13.0/24 {`
	`  default-router 192.168.13.254`
	`  dns-server 192.168.13.254`
	`  start 192.168.13.100 {`
	`  stop 192.168.13.200`
	`  }`
	`  }`
	`[edit]`
	`admin@edge#`

Вывод настройки интерфейсов.	`[edit]`
	`admin@edge# show interfaces`
	`  ethernet eth1 {`
	`  address 192.168.11.254/24`
	`  }`
	`  ethernet eth2 {`
	`  address 192.168.12.254/24`
	`  }`
	`  ethernet eth3 {`
	`  address 192.168.13.254/24`
	`  }`

35.2.2 Резервирование адресов

Бывают ситуации, когда конкретному узлу важно сопоставить конкретный IP-адрес вместо динамического назначения IP-адреса из пула адресов. Это называется резервированием.

Резервирование выполняется при помощи параметра static-mapping узла конфигурации подсети. В данном примере выполняется резервирование адресов в пуле, созданном в примере выше.

В примере ниже выполняется резервирование IP-адреса 192.168.11.100 для устройства с MAC-адресом 0c:ce:8b:51:00:00.

Пример 315- Резервирование адреса для клиента

Действие	Команда
Создание резерва с именем “lab” и ввод статического IP-адреса из диапазона для подсети 192.168.11.0/25.	[edit] admin@edge# set service dhcp-server subnet 192.168.11.0/24 static-mapping lab ip-address 192.168.11.100
Ввод соответствующего MAC-адреса для резерва из подсети 192.168.11.0/25.	[edit] admin@edge# set service dhcp-server subnet 192.168.11.0/24 static-mapping lab mac-address 0c:ce:8b:51:00:00
Фиксация изменений.	[edit] admin@edge# commit

Вывод настройки.	[edit]
	admin@edge# show service dhcp-server subnet 192.168.11.0/24
	default-router 192.168.11.254
	dns-server 192.168.11.254
	start 192.168.11.100 {
	stop 192.168.11.200
	}
	static-mapping lab {
	ip-address 192.168.11.100
	mac-address 0c:ce:8b:51:00:00
	}
	[edit]
	admin@edge#

Пример 316 - Просмотр аренды на DHCP сервере после резервирования IP адреса

Действие	Команда
Просмотр аренды на DHCP сервере после резервирования IP адреса	admin@edge:~$ service dhcp-server show leases IP address Hardware Address Lease expiration Subnet Client Name ---------- ---------- ------- --------- --------- ----------- 192.168.11.100 0c:ce:8b:51:00:00 10:23 2023-05-13 192.168.11.0/24 debian1 192.168.11.196 0c:ad:e6:35:00:00 10:23 2023-05-13 192.168.11.0/24 debian2 192.168.12.195 0c:9c:01:04:00:00 10:23 2023-05-13 192.168.12.0/24 debian3 192.168.12.140 0c:7c:52:e1:00:00 10:23 2023-05-13 192.168.12.0/24 debian4 192.168.13.107 0c:b2:22:b0:00:00 10:23 2023-05-13 192.168.13.0/24 debian5 192.168.13.111 0c:cc:e2:cd:00:00 10:23 2023-05-13 192.168.13.0/24 debian6

35.2.3 Настройка ретрансляции DHCP

Ретрансляция DHCP используется в тех случаях, когда у клиента DHCP нет возможности обратиться к серверу DHCP напрямую, в частности, если они находятся в разных широковещательных доменах. В этом случае

ретрансляция DHCP избавляет от необходимости установки и запуска DHCP сервера в каждом из широковещательных доменов.

В локальных сетях небольшого размера где все сетевые устройства находятся в одной подсети, клиенты DHCP могут обратиться напрямую к серверу DHCP, используя широковещательную рассылку. При этом сервер DHCP может быть настроен таким образом, чтобы выделять IP-адреса из нескольких подсетей. Однако в том случае если клиент и сервер DHCP расположены в различных подсетях, клиент не может обратиться напрямую к серверу DHCP, так как у него нет назначенного маршрутизируемого IP-адреса, а также ему неизвестен IP-адрес сервера DHCP. Для того чтобы клиенты, которые не находятся в одной подсети с сервером DHCP, могли к нему обращаться, необходимо настроить в данной подсети агент ретрансляции DHCP. В этом случае клиент DHCP отправляет широковещательный запрос с целью обнаружить доступные серверы DHCP, агент ретрансляции DHCP, получив данный запрос, передает его одному или нескольким серверам DHCP, используя индивидуальную рассылку (unicast). Агент ретрансляции при этом передает серверу IP-адрес интерфейса, на котором был получен запрос от клиента DHCP. На основании этого адреса сервер DHCP определяет из какой подсети необходимо выделить IP-адрес. Затем DHCP сервер формирует ответ клиенту и направляет его с использованием индивидуальной рассылки на адрес, который был передан ему агентом ретрансляции при передаче запроса. После чего агент ретрансляции передает ответ сервера DHCP клиенту при помощи широковещательной рассылки.

Удаленный сервер DHCP выдаст IP-адрес по запросу, полученному от агента ретрансляции только в том случае, если в настройке сервера определена область, включающая IP-адрес интерфейса агента ретрансляции, на котором был получен запрос от клиента DHCP.

Сервер DHCP направляет ответы на адрес интерфейса агента ретрансляции, на котором был получен запрос от клиента, таким образом, необходимо соответствующим образом настроить маршрутизацию на сервере DHCP, например, предварительно указав статический маршрут.

Дополнительно, на агенте ретрансляции может быть настроен параметр **service dhcp-relay <ip_клиентского_интерфейса> server-interface**, который определяет с какого интерфейса могут быть получены ответы от DHCP сервера. Данный параметр используется для защиты от спуфинга поддельных DHCP ответов полученных на недоверенном интерфейсе, например, смотрящем во внешнюю сеть.

ПРИМЕЧАНИЕ В конфигурации устройства могут одновременно присутствовать как сервер DHCP, так и агент ретрансляции, настроенные соответствующими командами разделов service dhcp-server и service dhcp-relay. В таком случае, при обработке запросов, поступающих с интерфейса, определенного в качестве клиентского для dhcp-relay, приоритет обработки будет у агента ретрансляции. Запрос клиента будет перенаправлен серверу DHCP, определенному настройками агента ретрансляции.

В данном разделе приведены следующие примеры:

- Пример 317 - Настройка ретрансляции DHCP
- Пример 318 - Настройка сервера DHCP
- Пример 319- Определение статического маршрута на сервере DHCP
- Пример 322 – Просмотр аренды на DHCP сервере

В результате выполнения данных примеров система будет настроена в соответствии с рисунком ниже.

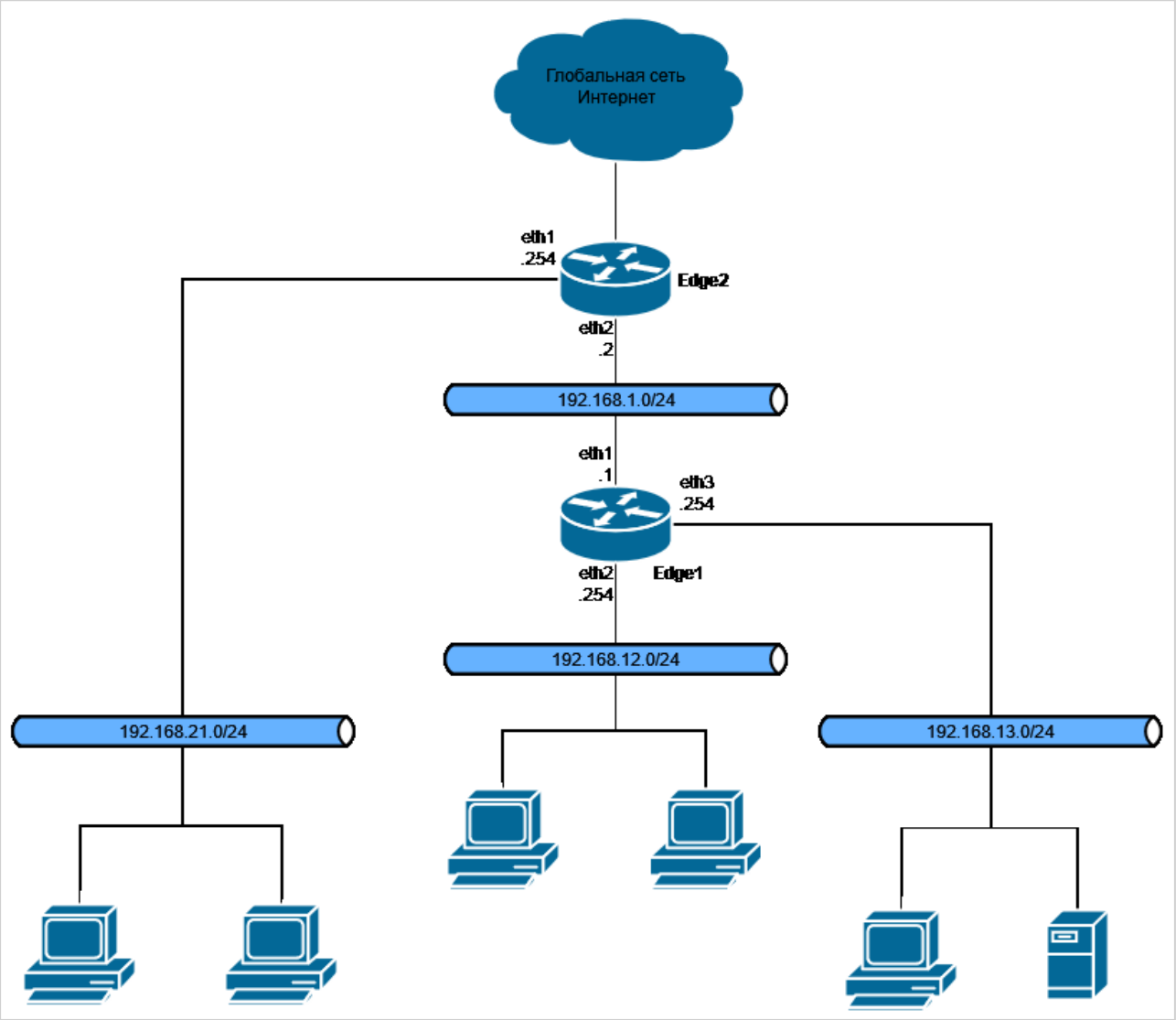


Рисунок 82 – Схема стенда

В примере 317 приведена настройка узла Edge1 в качестве агента ретрансляции DHCP.

Пример 317 - Настройка ретрансляции DHCP

Действие	**Команда**

Просмотр конфигурации интерфейсов ethernet на узле Edge1	[edit]
	admin@Edge1# show interfaces ethernet
	eth1 {
	address 192.168.1.1/24
	}
	eth2 {
	address 192.168.12.254/24
	}
	eth3 {
	address 192.168.13.254/24
	}
	[edit]
	admin@Edge1#

Создается узел конфигурации DCHP релея,где указывается IP-адрес интерфейса eth2.	[edit] admin@Edge1# set service dhcp-relay

Действие	Команда
	192.168.12.254
Далее указывается адрес DHCP сервера, на который будут перенаправляться запросы клиенов.	[edit] admin@Edge1# set service dhcp-relay 192.168.12.254 server-address 192.168.1.2
Затем указывается интерфейс, с которого ожидается получение ответов от DCHP сервера.	[edit] admin@Edge1# set service dhcp-relay 192.168.12.254 server-interface eth1
Аналогичным образом настраивается узел конфигурации для адреса 192.168.13.254, который настроен на интерфейсе eth3. Этот адрес используется в качестве адреса отправителя для отправки на DHCP сервер.	[edit] admin@Edge1# set service dhcp-relay 192.168.13.254
Указывается адрес DHCP сервера.	[edit] admin@Edge1# set service dhcp-relay 192.168.13.254 server-address 192.168.1.2
И интерфейс, смотрящий в сторону DHCP сервера. Если будет получен DHCP ответ с другого интерфейса, он будет отклонен.	[edit] admin@Edge1# set service dhcp-relay 192.168.13.254 server-interface eth1
Фиксация изменений.	[edit] admin@Edge1# commit

Просмотр получившейся конфигурации.	[edit]
	admin@Edge1# show service dhcp-relay
	192.168.12.254 {
	server-address 192.168.1.2
	server-interface eth1
	}
	192.168.13.254 {
	server-address 192.168.1.2
	server-interface eth1
	}
	[edit]
	admin@Edge1#

В примере 318 приведена настройка узла Edge2 в качестве сервера DHCP.

Пример 318 - Настройка сервера DHCP

Действие	Команда

Просмотр конфигурации интерфейсов на узле Edge2.	[edit]
	admin@Edge2# show interfaces ethernet
	eth1 {
	address 192.168.21.254/24
	}
	eth2 {
	address 192.168.1.2/24
	}
	[edit]
	admin@Edge2#

Создание узла конфигурации для подсети	[edit]

Действие	**Команда**
192.168.21.0/24. Ввод начального и конечного IP-адресов для пула.	`admin@Edge2# set service dhcp-server subnet 192.168.21.0/24 start 192.168.21.100 stop 192.168.21.200`
Ввод маршрутизатора по умолчанию для клиентов подсети 192.168.21.0/24.	`[edit]` `admin@Edge2# set service dhcp-server subnet 192.168.21.0/24 default-router 192.168.21.254`
Ввод сервера DNS для клиентов подсети 192.168.21.0/24.	`[edit]` `admin@Edge2# set service dhcp-server subnet 192.168.21.0/24 dns-server 192.168.21.254`
Создание узла конфигурации для подсети 192.168.12.0/24. Ввод начального и конечного IP-адресов для пула.	`[edit]` `admin@Edge2# set service dhcp-server subnet 192.168.12.0/24 start 192.168.12.100 stop 192.168.12.200`
Ввод маршрутизатора по умолчанию для клиентов подсети 192.168.12.0/24.	`[edit]` `admin@Edge2# set service dhcp-server subnet 192.168.12.0/24 default-router 192.168.12.254`
Ввод сервера DNS для клиентов подсети 192.168.12.0/24.	`[edit]` `admin@Edge2# set service dhcp-server subnet 192.168.12.0/24 dns-server 192.168.12.254`
Создание узла конфигурации для подсети 192.168.13.0/24. Ввод начального и конечного IP-адресов для пула.	`[edit]` `admin@Edge2# set service dhcp-server subnet 192.168.13.0/24 start 192.168.13.100 stop 192.168.13.200`
Ввод маршрутизатора по умолчанию для клиентов подсети 192.168.13.0/24.	`[edit]` `admin@Edge2# set service dhcp-server subnet 192.168.13.0/24 default-router 192.168.13.254`
Ввод сервера DNS для клиентов подсети 192.168.13.0/24.	`[edit]` `admin@Edge2# set service dhcp-server subnet 192.168.13.0/24 dns-server 192.168.13.254`
Фиксация настройки.	`[edit]` `admin@Edge2# commit`

Вывод настройки	`[edit]`
	`admin@Edge2# show service dhcp-server`
	`  subnet 192.168.12.0/24 {`
	`  default-router 192.168.12.254`
	`  dns-server 192.168.12.254`
	`  start 192.168.12.100 {`
	`  stop 192.168.12.200`
	`  }`
	`  }`
	`  subnet 192.168.13.0/24 {`
	`  default-router 192.168.13.254`
	`  dns-server 192.168.13.254`

Действие	Команда

	start 192.168.13.100 {
	stop 192.168.13.200
	}
	}
	subnet 192.168.21.0/24 {
	default-router 192.168.21.254
	dns-server 192.168.21.254
	start 192.168.21.100 {
	stop 192.168.21.200
	}
	}
	[edit]
	admin@Edge2#

В примере 319 приведено определение статических маршрутов к удаленным подсетям на сервере DHCP.

Так как на участке между агентом ретрансляции и DHCP сервером используется индивидуальная рассылка, то получателем пакета от сервера будет указан адрес, назначенный клиентскому интерфейсу агента ретрансляции. Там образом на DHCP сервере потребуется указать статические маршруты до подсетей 192.168.12.0/24 и 192.168.13.0/24 с адресом 192.168.1.1 в качестве следующего транзитного узла для трафика. Для этого необходимо выполнить следующие действия в режиме настройки:

Пример 319- Определение статического маршрута на сервере DHCP

Действие	Команда
Создание статического маршрута к подсети 192.168.12.0/24.	[edit] admin@Edge2# set protocols static route 192.168.12.0/24 next-hop 192.168.1.1
Создание статического маршрута к подсети 192.168.13.0/24.	[edit] admin@Edge2# set protocols static route 192.168.13.0/24 next-hop 192.168.1.1
Фиксация настройки.	[edit] admin@Edge2# commit

Отображение настройки.	[edit]
	admin@Edge2# show protocols
	static {
	route 192.168.12.0/24 {
	next-hop 192.168.1.1 {
	}
	}
	route 192.168.13.0/24 {
	next-hop 192.168.1.1 {
	}
	}
	}
	[edit]
	admin@Edge2#

Пример 320 - Просмотр аренды на DHCP сервере

Действие	Команда
Просмотр аренды на DHCP сервере	admin@Edge2:~$ service dhcp-server show leases IP address Hardware Address Lease expiration Subnet Client Name ---------- ---------- ---------- ------- --------- ----------- 192.168.12.152 0c:c8:c3:f7:00:00 12:07 2023-05-13 192.168.12.0/24 debian4 192.168.12.100 0c:55:1d:f9:00:00 12:07 2023-05-13 192.168.12.0/24 debian3 192.168.13.107 0c:57:59:26:00:00 11:59 2023-05-13 192.168.13.0/24 debian5 192.168.13.190 0c:1d:10:c3:00:00 11:59 2023-05-13 192.168.13.0/24 debian6 192.168.21.179 0c:d1:2f:c2:00:00 11:51 2023-05-13 192.168.21.0/24 debian2 192.168.21.143 0c:ba:50:c8:00:00 11:53 2023-05-13 192.168.21.0/24 debian1

35.3 Команды DHCP

Таблица 271 - Команды DHCP

Команды настройки сервера DHCP	
service dhcp-server	Включение функциональности сервера DHCP.
service dhcp-server authoritative <состояние>	Указание авторитетности сервера DHCP.
service dhcp-server subnet <подсеть_ipv4>	Включает DHCP сервер для указанной подсети.
service dhcp-server subnet <подсеть_ipv4> active <состояние>	Возможность отключения сервера DHCP для указанной подсети с сохранением настройки.
service dhcp-server subnet <подсеть_ipv4> bootfile-name <имя_файла>	Указание файла начальной загрузки, из которого могут загружаться бездисковые ПК.
service dhcp-server subnet <подсеть_ipv4> bootfile-server <адрес>	Указание сервера начальной загрузки, с которого могут загружаться бездисковые ПК.
service dhcp-server subnet <подсеть_ipv4> client-prefix-length <префикс>	Указание длины префикса подсети, назначаемой клиентам.
service dhcp-server subnet <подсеть_ipv4> default-router <адрес>	Указание маршрутизатора по умолчанию для клиентов DHCP в данной подсети.
service dhcp-server subnet <подсеть_ipv4> description <текст>	Указание текстового описания для определенной подсети.
service dhcp-server subnet <подсеть_ipv4> dns-server <адрес>	Указание сервера DNS для клиентов DHCP.
service dhcp-server subnet <подсеть_ipv4> domain-name <имя_домена>	Ввод имени домена для клиентов DHCP.
service dhcp-server subnet <подсеть_ipv4> lease <секунды>	Указание времени аренды адреса, назначенного сервером DHCP.
service dhcp-server subnet <подсеть_ipv4> next-server <адрес>	Указание адреса вспомогательного сервера для клиентов DHCP.
service dhcp-server subnet <подсеть_ipv4> ntp server <адрес>	Указание адреса сервера протокола NTP, доступного для клиентов.
service dhcp-server subnet <подсеть_ipv4> pop-server <адрес>	Указание адреса сервера протокола POP3, доступного для клиентов.

service dhcp-server subnet <подсеть_ipv4> server-identifier <адрес>	Указание адреса идентифицирующего сервер DHCP.
service dhcp-server subnet <подсеть_ipv4> smtp-server <адрес>	Указание адреса сервера протокола SMTP, доступного для клиентов.
service dhcp-server subnet <подсеть_ipv4> start <адрес> stop < адрес>	Указание диапазона адресов, которые будут назначаться клиентам DHCP.
service dhcp-server subnet <подсеть_ipv4> static-mapping <имя_резерва>	Название резерва IP-адреса для клиента.
service dhcp-server subnet <подсеть_ipv4> static-mapping <имя_резерва> disable	Временное отключение резерва IP для клиента.
service dhcp-server subnet <подсеть_ipv4> static-mapping <имя_резерва> ip-address <адрес>	Указание статического IP-адреса для конкретного клиента DHCP.
service dhcp-server subnet <подсеть_ipv4> static-mapping <имя_резерва> mac-address <адрес>	Указание MAC-адреса клиента DHCP, которому нужно назначить статический IP-адрес.
service dhcp-server subnet <подсеть_ipv4> static-route destination-subnet <подсеть_ipv4> gateway <адрес>	Указание шлюза для статического маршрута, передаваемого клиентам.
service dhcp-server subnet <подсеть_ipv4> tftp-server-name <имя_сервера>	Указание имени сервера протокола TFTP, доступного для клиентов.
service dhcp-server subnet <подсеть_ipv4> time-offset <секунды>	Указание сдвига времени в клиентской подсети от гринвичского (координированного всемирного) времени.
service dhcp-server subnet <подсеть_ipv4> time-server <адрес>	Указание адреса сервера времени RFC868, доступного для клиентов.
service dhcp-server subnet <подсеть_ipv4> wins-server <адрес>	Указание адреса сервера WINS, доступного для клиентов DHCP.
service dhcp-server subnet <подсеть_ipv4> wpad-url <адрес>	Указание URL-адреса службы автоопределения веб-прокси (WPAD).
Ретрансляция DHCP	
service dhcp-relay <ip_клиентского_интерфейса>	Настройка системы в качестве агента ретрансляции DHCP.
service dhcp-relay <ip_клиентского_интерфейса> server-interface <интерфейс>	Указание интерфейса, через который запросы от клиентов DHCP будут передаваться на сервер DHCP.
service dhcp-relay <ip_клиентского_интерфейса> server-address <адрес>	Указание IP-адреса сервера DHCP, которому будут передаваться запросы от клиентов DHCP.
service dhcp-relay <ip_клиентского_интерфейса> active <состояние>	Возможность отключения ретрансляции DHCP с сохранением настройки.
Эксплуатационные команды	
service dhcp-client release interface <интерфейс>	Освобождение текущей аренды клиента DHCP на интерфейсе.
service dhcp-client renew interface <интерфейс>	Обновление текущей аренды клиента DHCP на интерфейсе.
service dhcp-client show leases	Отображение сведений DHCP для интерфейсов, настроенных как клиенты DHCP.
service dhcp-server show leases	Отображение информации о выделенных адресах DHCP сервером.

35.3.1 service dhcp-server

Включение функциональности сервера DHCP.

Синтаксис

```
set service dhcp-server
delete service dhcp-server
show service dhcp-server
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dhcp-server {
   }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для включения службы DHCP.

Для того чтобы DHCP был доступен как служба, должен быть настроен как минимум один пул адресов. Каждая указанная подсеть содержит отдельный пул адресов. На одном интерфейсе может поддерживаться несколько пулов адресов (то есть более одной подсети).

Форма **set** этой команды используется для включения функциональности сервера DHCP.

Форма **delete** этой команды используется для удаления функциональности сервера DHCP.

Форма **show** этой команды используется для просмотра настройки сервера DHCP.

35.3.2 service dhcp-server authoritative <состояние>

Указание авторитетности сервера DHCP.

Синтаксис

```
set service dhcp-server authoritative <состояние>
delete service dhcp-server authoritative
show service dhcp-server authoritative
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dhcp-server {
      authoritative состояние
   }
}
```

Параметры

состояние

Указание авторитетности сервера DHCP. Поддерживаются следующие значения:

enable: состояние включено.

disable: состояние отключено.

Значение по умолчанию

Сервер DHCP не является авторитетным.

Указания по использованию

Эта команда используется для установки сервера в качестве авторитетного сервера DHCP.

Установка сервера в качестве авторитетного делает его главным сервером и позволяет ему защититься от неавторизованных серверов DHCP или неправильно настроенных клиентов DHCP. Если сервер является авторитетным, он отправляет сообщение DHCPNAK неправильно настроенному клиенту; в противном случае клиент не сможет обновить свой IP-адрес до истечения срока текущей аренды.

Форма **set** этой команды используется для включения или отключения авторитетного состояния для сервера DHCP.

Форма **delete** этой команды используется для восстановления авторитетного состояния по умолчанию.

Форма **show** этой команды используется для просмотра настройки авторитетности DHCP.

35.3.3 service dhcp-server subnet <подсеть_ipv4>

Включает DHCP сервер для указанной подсети.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4>
delete service dhcp-server subnet <подсеть_ipv4>
show service dhcp-server subnet <подсеть_ipv4>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dhcp-server {
      subnet подсеть_ipv4 {
      }
   }
}
```

Параметры

подсеть_ipv4

Множественный узел. Подсеть IPv4, на которой юудет работать DHCP сервер. Формат – ipv4-адрес/префикс.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания подсети IPv4, на которой будет работать DHCP сервер. DHCP запросы от устройств из этой подсети обслуживаются адресами заданного пула или статическим назначением адресов.

Форма **set** этой команды используется для включения DHCP сервера для указанной подсети.

Форма **delete** этой команды используется для удаления DHCP сервера для указанной подсети.

Форма **show** этой команды используется для просмотра настройки DHCP сервера для указанной подсети.

35.3.4 service dhcp-server subnet <подсеть_ipv4> active <состояние>

Возможность отключения сервера DHCP для указанной подсети с сохранением настройки.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> active <состояние>
delete service dhcp-server subnet <подсеть_ipv4> active
show service dhcp-server subnet <подсеть_ipv4> active
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dhcp-server {
      subnet подсеть_ipv4 {
         active состояние
      }
   }
}
```

Параметры

состояние

Административное состояние сервера DHCP для указанной подсети. Поддерживаются следующие значения:

on: Включение сервера DHCP.

off: Отключение сервера DHCP без отбрасывания настройки.

Значение по умолчанию

Функциональность сервера DHCP включена.

Указания по использованию

Эта команда используется для отключения сервера DHCP для указанной подсети с сохранением настройки.

Форма **set** этой команды используется, чтобы указать, будет сервер DHCP отключен или нет.

Форма **delete** этой команды используется для восстановления состояния по умолчанию.

Форма **show** этой команды используется для просмотра состояния сервера DHCP.

35.3.5 service dhcp-server subnet <подсеть_ipv4> bootfile-name <имя_файла>

Указание файла начальной загрузки, который могут использовать устройства без загрузочного образа.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> bootfile-name <имя_файла>
delete service dhcp-server subnet <подсеть_ipv4> bootfile-name
show service dhcp-server subnet <подсеть_ipv4> bootfile-name
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dhcp-server {
      subnet подсеть_ipv4 {
         bootfile-name имя_файла
      }
   }
}
```

Параметры

подсеть_ipv4

Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

имя_файла

Имя файла начальной загрузки, используемого для загрузки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания файла начальной загрузки, который могут использовать устройства без загрузочного образа.

Форма **set** этой команды может использоваться для указания файла начальной загрузки.

Форма **delete** этой команды может использоваться для удаления настройки файла начальной загрузки.

Форма **show** этой команды может использоваться для просмотра настройки файла начальной загрузки.

35.3.6 service dhcp-server subnet <подсеть_ipv4> bootfile-server <адрес>

Указание сервера начальной загрузки, с помощью которого могут запускаться устройства без загрузочного образа.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> bootfile-server <адрес>
delete service dhcp-server subnet <подсеть_ipv4> bootfile-server
show service dhcp-server subnet <подсеть_ipv4> bootfile-server
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dhcp-server {
      subnet подсеть_ipv4 {
         bootfile-server адрес
      }
   }
}
```

Параметры

подсеть_ipv4

Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

адрес

IPv4-адрес сервера, хранящего файл начальной загрузки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания сервера начальной загрузки, с помощью которого могут запускаться устройства без загрузочного образа..

Форма **set** этой команды используется для указания сервера начальной загрузки.

Форма **delete** этой команды используется для удаления настройки сервера начальной загрузки.

Форма **show** этой команды используется для просмотра настройки сервера начальной загрузки.

35.3.7 service dhcp-server subnet <подсеть_ipv4> client-prefix-length <префикс>

Указание длины префикса подсети, назначаемой клиентам.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> client-prefix-length <префикс>
```

```
delete service dhcp-server subnet <подсеть_ipv4> client-prefix-length
show service dhcp-server subnet <подсеть_ipv4> client-prefix-length
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    dhcp-server {
        subnet подсеть_ipv4 {
            client-prefix-length префикс
        }
    }
}
```

Параметры

подсеть_ipv4

Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

префикс

Длина префикса подсетей. Данное значение будет назначено каждому клиенту. Значение должно находиться в диапазоне от 0 до 32.

Значение по умолчанию

По умолчанию назначается значение длины префикса, определенное в параметре subnet.

Указания по использованию

Эта команда используется для указания длины префикса подсети, назначаемой клиентам.

Форма **set** этой команды используется для указания длины префикса подсети, назначаемой клиентам.

Форма **delete** этой команды используется для удаления настройки client-prefix-length.

Форма **show** этой команды используется для просмотра настройки client-prefix-length.

35.3.8 service dhcp-server subnet <подсеть_ipv4> default-router <адрес>

Указание маршрутизатора по умолчанию для клиентов DHCP в данной подсети.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> default-router <адрес>
delete service dhcp-server subnet <подсеть_ipv4> default-router
show service dhcp-server subnet <подсеть_ipv4> default-router
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    dhcp-server {
        subnet подсеть_ipv4 {
            default-router адрес
        }
    }
}
```

Параметры

подсеть_ipv4

Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

адрес

IPv4-адрес маршрутизатора по умолчанию для клиентов DHCP в данной подсети. Маршрутизатор по умолчанию должен быть расположен в той же подсети, что и клиент.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания адреса маршрутизатора (шлюза) по умолчанию для клиентов DHCP в данной подсети.

Форма **set** этой команды используется для указания адреса маршрутизатора по умолчанию для клиентов DHCP в данной подсети.

Форма **delete** этой команды используется для удаления конфигурации default-router.

Форма **show** этой команды используется для просмотра конфигурации default-router.

35.3.9 service dhcp-server subnet <подсеть_ipv4> description <текст>

Указание текстового описания для определенной подсети.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> description <текст>
delete service dhcp-server subnet <подсеть_ipv4> description <текст>
show service dhcp-server subnet <подсеть_ipv4> description
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dhcp-server {
      subnet подсеть_ipv4 {
         description текст
      }
   }
}
```

Параметры

подсеть_ipv4

Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

текст

Текстовое описание указанной подсети.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания текстового описания подсети в системе конфигурации.

Форма **set** этой команды используется для указания текстового описания подсети.

Форма **delete** этой команды используется для удаления текстового описания подсети.

Форма **show** этой команды используется для просмотра текстового описания подсети.

35.3.10 service dhcp-server subnet <подсеть_ipv4> dns-server <адрес>

Указание сервера DNS для клиентов DHCP.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> dns-server <адрес>
delete service dhcp-server subnet <подсеть_ipv4> dns-server <адрес>
show service dhcp-server subnet <подсеть_ipv4> dns-server
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dhcp-server {
      subnet подсеть_ipv4 {
         dns-server адрес
      }
   }
}
```

Параметры

подсеть_ipv4

Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

адрес

Множественный узел. IPv4-адрес сервера DNS. Можно указать более одного сервера DNS, выдав эту команду несколько раз.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания адреса сервера DNS, доступного для клиентов DHCP.

Форма **set** этой команды используется для указания адреса сервера DNS, доступного клиентам DHCP.

Форма **delete** этой команды используется для удаления настройки сервера DNS.

Форма **show** этой команды используется для просмотра настройки сервера DNS.

35.3.11 service dhcp-server subnet <подсеть_ipv4> domain-name <имя_домена>

Ввод имени домена для клиентов DHCP.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> domain-name <имя_домена>
delete service dhcp-server subnet <подсеть_ipv4> domain-name
show service dhcp-server subnet <подсеть_ipv4> domain-name
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dhcp-server {
```

```
        subnet подсеть_ipv4 {
            domain-name имя_домена
        }
    }
}
```

Параметры

подсеть_ipv4

Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

имя_домена

Имя домена, которое должно быть выдано клиентам DHCP в этой сети. В состав имени домена могут входить буквы, цифры, дефисы (“-”) и одна точка (“.”). Например, “example.com”.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания имени домена, которое будет использоваться клиентами DHCP в данной подсети.

Форма **set** этой команды используется для указания имени домена для клиентов.

Форма **delete** этой команды используется для удаления настройки имени домена для клиентов.

Форма **show** этой команды используется для просмотра настройки имени домена для клиентов.

35.3.12 service dhcp-server subnet <подсеть_ipv4> lease <секунды>

Указание времени действительности адреса, назначенного сервером DHCP.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> lease <время>
delete service dhcp-server subnet <подсеть_ipv4> lease
show service dhcp-server subnet <подсеть_ipv4> lease
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    dhcp-server {
        subnet подсеть_ipv4 {
            lease время
        }
    }
}
```

Параметры

подсеть_ipv4

Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

время

Указание времени (в секундах) действительности адреса, назначенного сервером DHCP. Диапазон допустимых значений составляет 0-4294967295.

Значение по умолчанию

Значение по умолчанию равно 86400 (24 часа).

Указания по использованию

Эта команда используется для указания времени действительности адреса, назначенного сервером DHCP.

Форма **set** этой команды используется для указания времени действительности адреса, назначенного сервером DHCP.

Форма **delete** используется для удаления конфигурации аренды.

Форма **show** этой команды используется для просмотра конфигурации аренды.

35.3.13 service dhcp-server subnet <подсеть_ipv4> next-server <адрес>

Указание адреса вспомогательного сервера.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> next-server <адрес>
delete service dhcp-server subnet <подсеть_ipv4> next-server <адрес>
show service dhcp-server subnet <подсеть_ipv4> next-server
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dhcp-server {
      subnet подсеть_ipv4 {
         next-server адрес
      }
   }
}
```

Параметры

подсеть_ipv4

Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

адрес

IPv4-адрес вспомогательного сервера. Указание адреса для идентификатора сервера DHCP.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания адреса вспомогательного сервера, доступного для клиентов.

Форма **set** этой команды используется для указания вспомогательного адреса сервера.

Форма **delete** этой команды используется для удаления конфигурации вспомогательного сервера.

Форма **show** этой команды используется для просмотра конфигурации вспомогательного сервера.

35.3.14 service dhcp-server subnet <подсеть_ipv4> ntp server <адрес>

Указание адреса сервера протокола NTP, доступного для клиентов.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> ntp-server <адрес>
delete service dhcp-server subnet <подсеть_ipv4> ntp-server <адрес>
```

```
show service dhcp-server subnet <подсеть_ipv4> ntp-server
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    dhcp-server {
        subnet подсеть_ipv4 {
            ntp-server адрес
        }
    }
}
```

Параметры

подсеть_ipv4

Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

адрес

Указание IPv4-адреса сервера протокола NTP, доступного для клиентов. Можно указать несколько адресов серверов NTP отдельными командами. Список серверов NTP следует указывать в порядке предпочтительности.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания адреса сервера NTP, доступного для клиентов.

Форма **set** этой команды используется для указания адреса сервера NTP, доступного для клиентов.

Форма **delete** этой команды используется для удаления конфигурации сервера NTP.

Форма **show** этой команды используется для просмотра конфигурации сервера NTP.

35.3.15 service dhcp-server subnet <подсеть_ipv4> pop-server <адрес>

Указание адреса сервера протокола POP3, доступного для клиентов.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> pop-server <адрес>
delete service dhcp-server subnet <подсеть_ipv4> pop-server <адрес>
show service dhcp-server subnet <подсеть_ipv4> pop-server
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    dhcp-server {
        subnet подсеть_ipv4 {
            pop-server адрес
        }
    }
}
```

Параметры

подсеть_ipv4

Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

адрес

Указание IPv4-адреса сервера протокола POP3, доступного для клиентов. Можно указать несколько адресов серверов POP3 отдельными командами. Список серверов POP3 следует указывать в порядке предпочтительности.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания адреса сервера POP3, доступного для клиентов.

Форма **set** этой команды используется для указания адреса сервера POP3, доступного для клиентов.

Форма **delete** этой команды используется для удаления конфигурации сервера POP3.

Форма **show** этой команды используется для просмотра конфигурации сервера POP3.

35.3.16 service dhcp-server subnet <подсеть_ipv4> server-identifier <адрес>

Указание адреса идентифицирующего сервер DHCP.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> server-identifier <адрес>
delete service dhcp-server subnet <подсеть_ipv4> server-identifier
show service dhcp-server subnet <подсеть_ipv4> server-identifier
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dhcp-server {
      subnet подсеть_ipv4 {
         server-identifier адрес
      }
   }
}
```

Параметры

подсеть_ipv4

Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

адрес

Указание IPv4-адреса для идентификатора сервера DHCP.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания адреса идентифицирующего сервер DHCP. Необязательный параметр идентификатора сервера — это поле в сообщении DHCP, идентифицирующее сервер DHCP как адрес получателя пакетов, отправляемых с клиентов на сервер. Если сервер DHCP включает это поле в пакет DHCPOffer, клиент может использовать его, чтобы отличать друг от друга несколько предложений аренды. Идентификатор сервера должен содержать адрес, достижимым с клиента.

Форма **set** этой команды используется для указания адреса идентифицирующего сервер DHCP.

Форма **delete** этой команды используется для удаления адреса идентифицирующего сервер DHCP.

Форма **show** этой команды используется для просмотра конфигурации идентификатора сервера DHCP.

35.3.17 service dhcp-server subnet <подсеть_ipv4> smtp-server <адрес>

Указание адреса сервера протокола SMTP, доступного для клиентов.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> smtp-server <адрес>
delete service dhcp-server subnet <подсеть_ipv4> smtp-server <адрес>
show service dhcp-server subnet <подсеть_ipv4> smtp-server
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dhcp-server {
      subnet подсеть_ipv4 {
         smtp-server адрес
      }
   }
}
```

Параметры

подсеть_ipv4

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

адрес

Необязательный параметр. Указание IPv4-адреса сервера протокола SMTP, доступного для клиентов. Можно указать несколько адресов серверов SMTP отдельными командами. Список серверов SMTP следует указывать в порядке предпочтительности.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания адреса сервера SMTP, доступного для клиентов.

Форма **set** этой команды используется для указания адреса сервера SMTP, доступного для клиентов.

Форма **delete** этой команды используется для удаления конфигурации сервера SMTP.

Форма **show** этой команды используется для просмотра конфигурации сервера SMTP.

35.3.18 service dhcp-server subnet <подсеть_ipv4> start <адрес> stop < адрес>

Указание диапазона адресов, которые будут назначаться клиентам DHCP.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> start <адрес> stop <адрес>
delete service dhcp-server subnet <подсеть_ipv4> start [<адрес> [stop]]
show service dhcp-server subnet <подсеть_ipv4> start
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    dhcp-server {
        subnet подсеть_ipv4 {
            start адрес {
                stop адрес
            }
        }
    }
}
```

Параметры

подсеть_ipv4

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

start *адрес*

Необязательный параметр. Множественный узел. Начальный адрес в диапазоне адресов. Это первый адрес в диапазоне, из которого могут назначаться адреса. Для одной подсети можно определить несколько диапазонов адресов, создав несколько узлов конфигурации start. Формат – ipv4-адрес.

stop *адрес*

Обязательный параметр. Конечный адрес в диапазоне адресов. Это последний адрес в диапазоне, из которого могут назначаться адреса. Формат – ipv4-адрес.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания диапазона назначаемых клиентам адресов.

Форма **set** этой команды используется для указания диапазона назначаемых клиентам адресов.

Форма **delete** этой команды используется для удаления конфигурации диапазона адресов.

Форма **show** этой команды используется для просмотра конфигурации диапазона адресов.

35.3.19 service dhcp-server subnet <подсеть_ipv4> static-mapping <имя_резерва>

Название резерва IP-адреса для клиента.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> static-mapping <имя_резерва>
delete service dhcp-server subnet <подсеть_ipv4> static-mapping <имя_резерва>
show service dhcp-server subnet <подсеть_ipv4> static-mapping <имя_резерва>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    dhcp-server {
        subnet подсеть_ipv4 {
            static-mapping имя_резерва {
            }
```

```
        }
    }
}
```

Параметры

подсеть_ipv4

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

имя_резерва

Необязательный параметр. Множественный узел. Имя для резерва IP-адреса. Можно определить несколько резервов, создав несколько узлов конфигурации static-mapping.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для создания резерва IP-адреса. Резервирование позволяет создать статическое соответствие между конкретным клиентом DHCP (определяемым по его MAC-адресу) и назначаемым ему IP-адресом.

Форма **set** этой команды используется для определения резерва IP-адреса.

Форма **delete** этой команды используется для удаления резерва IP-адреса.

Форма **show** этой команды используется для просмотра настройки резервирования.

35.3.20 service dhcp-server subnet <подсеть_ipv4> static-mapping <имя_резерва> disable

Временное отключение резерва IP для клиента.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> static-mapping <имя_резерва> disable
delete service dhcp-server subnet <подсеть_ipv4> static-mapping <имя_резерва> disable
show service dhcp-server subnet <подсеть_ipv4> static-mapping <имя_резерва>
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    dhcp-server {
        subnet подсеть_ipv4 {
            static-mapping имя_резерва {
                disable
            }
        }
    }
}
```

Параметры

подсеть_ipv4

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

имя_резерва

Необязательный параметр. Множественный узел. Имя для резерва IP-адреса. Можно определить несколько резервов, создав несколько узлов конфигурации static-mapping.

Значение по умолчанию

Резервирование включено.

Указания по использованию

Эта команда используется для отключения настройки конкретного резерва IP без удаления настройки.

Форма **set** этой команды используется для временного отключения резервирования IP.

Форма **delete** этой команды используется для включения резервирования IP.

Форма **show** этой команды используется для просмотра настройки временного отключения резервирования.

35.3.21 service dhcp-server subnet <подсеть_ipv4> static-mapping <имя_резерва> ip-address <адрес>

Указание статического IP-адреса для конкретного клиента DHCP.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> static-mapping <имя_резерва> ip-address <адрес>

delete service dhcp-server subnet <подсеть_ipv4> static-mapping <имя_резерва> ip-address

show service dhcp-server subnet <подсеть_ipv4> static-mapping <имя_резерва> ip-address
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    dhcp-server {
        subnet подсеть_ipv4 {
            static-mapping имя_резерва {
                ip-address адрес
            }
        }
    }
}
```

Параметры

подсеть_ipv4

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

имя_резерва

Множественный узел. Имя для резерва IP-адреса. Можно определить несколько резервов, создав несколько узлов конфигурации static-mapping.

адрес

Обязательный параметр. IPv4-адрес, который должен быть статически назначен устройству.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания статического IP-адреса для конкретного клиента DHCP, определяемого его MAC-адресом.

Форма **set** этой команды используется для указания статического IP-адреса для конкретного клиента DHCP, определяемого его MAC-адресом.

Форма **delete** этой команды используется для удаления настройки статического сопоставления.

Форма **show** этой команды используется для просмотра настройки статического сопоставления.

35.3.22 service dhcp-server subnet <подсеть_ipv4> static-mapping <имя_резерва> mac-address <адрес>

Указание MAC-адреса клиента DHCP, которому нужно назначить статический IP-адрес.

Синтаксис

```
set service dhcp-server subnet подсеть_ipv4 static-mapping <имя_резерва> mac-address <адрес>

delete service dhcp-server subnet подсеть_ipv4 static-mapping <имя_резерва> mac-address

show service dhcp-server subnet подсеть_ipv4 static-mapping <имя_резерва> mac-address
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    dhcp-server {
        subnet подсеть_ipv4 {
            static-mapping имя_резерва {
                mac-address адрес
            }
        }
    }
}
```

Параметры

подсеть_ipv4

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

имя_резерва

Множественный узел. Имя для резерва IP-адреса. Можно определить несколько резервов, создав несколько узлов конфигурации static-mapping.

адрес

Обязательный параметр. MAC-адрес, который следует статически сопоставить с указанным IP-адресом.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания MAC-адреса клиента DHCP, которому следует назначить IP-адрес.

Форма **set** этой команды используется для указания MAC-адреса клиента DHCP.

Форма **delete** этой команды используется для удаления настройки резервирования.

Форма **show** этой команды используется для просмотра настройки резервирования.

35.3.23 service dhcp-server subnet <подсеть_ipv4> static-route destination-subnet <подсеть_ipv4> gateway <адрес>

Указание шлюза для статического маршрута, передаваемого клиентам.

Синтаксис

```
set service dhcp-server subnet подсеть_ipv4 static-route destination-subnet подсеть_ipv4 gateway адрес

delete service dhcp-server subnet подсеть_ipv4 static-route destination-subnet

show service dhcp-server subnet подсеть_ipv4 static-route destination-subnet подсеть_ipv4 gateway адрес
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    dhcp-server {
        subnet подсеть_ipv4 {
            static-route {
                destination-subnet подсеть_ipv4 {
                    gateway адрес
                }
            }
        }
    }
}
```

Параметры

subnet *подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

destination-subnet *подсеть_ipv4*

Необязательный параметр. Множественный параметр. Подсеть назначения для статического маршрута, передаваемого для сохранения в таблицах маршрутизации клиентов. Формат – ipv4-адрес/префикс.

адрес

Обязательный параметр. IPv4-адрес шлюза для целевой подсети статического маршрута, который следует использовать клиентам для доступа к ней.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания статических маршрутов, доступных клиентам. Указывается сеть назначения и шлюз (адрес маршрутизатора) для доступа к ней.

Форма **set** этой команды используется для указания подсети назначения и шлюза статического маршрута.

Форма **delete** этой команды используется для удаления настройки статической маршрутизации.

Форма **show** этой команды используется для просмотра настройки статической маршрутизации.

35.3.24 service dhcp-server subnet <подсеть_ipv4> tftp-server-name <имя_сервера>

Указание имени сервера протокола TFTP, доступного для клиентов.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> tftp-server-name <имя_сервера>
delete service dhcp-server subnet <подсеть_ipv4> tftp-server-name
show service dhcp-server subnet <подсеть_ipv4> tftp-server-name
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dhcp-server {
      subnet подсеть_ipv4 {
         tftp-server-name имя_сервера
      }
   }
}
```

Параметры

подсеть_ipv4

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

имя_сервера

Имя сервера TFTP, доступного для клиентов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания имени сервера TFTP, доступного для клиентов.

Форма **set** этой команды используется для указания имени сервера TFTP, доступного для клиентов.

Форма **delete** этой команды используется для удаления настройки сервера TFTP.

Форма **show** этой команды используется для просмотра настройки сервера TFTP.

35.3.25 service dhcp-server subnet <подсеть_ipv4> time-offset <секунды>

Указание сдвига времени в клиентской подсети от гринвичского (координированного всемирного) времени.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> time-offset <секунды>
delete service dhcp-server subnet <подсеть_ipv4> time-offset
show service dhcp-server subnet <подсеть_ipv4> time-offset
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dhcp-server {
```

```
        subnet подсеть_ipv4 {
            time-offset секунды
        }
    }
}
```

Параметры

подсеть_ipv4

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

секунды

Указание сдвига времени в клиентской подсети от гринвичского (координированного всемирного) времени. Допустимые форматы указания времени: -<секунды>; <секунды>.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания сдвига времени в клиентской подсети от гринвичского (координированного всемирного) времени.

Форма **set** этой команды используется для указания сдвига времени в клиентской подсети от гринвичского (координированного всемирного) времени.

Форма **delete** этой команды используется для удаления настройки сдвига времени.

Форма **show** этой команды используется для просмотра настройки сдвига времени.

35.3.26 service dhcp-server subnet <подсеть_ipv4> time-server <адрес>

Указание адреса сервера времени RFC868, доступного для клиентов.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> time-server <адрес>
delete service dhcp-server subnet <подсеть_ipv4> time-server <адрес>
show service dhcp-server subnet <подсеть_ipv4> time-server
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    dhcp-server {
        subnet подсеть_ipv4 {
            time-server адрес
        }
    }
}
```

Параметры

подсеть_ipv4

Формат – ipv4-адрес/префикс. Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP.

адрес

Необязательный параметр. Указание IPv4-адреса сервера времени RFC868, доступного для клиентов. Можно указать несколько адресов серверов времени отдельными командами. Список серверов времени следует указывать в порядке предпочтительности.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания адреса сервера времени RFC868, доступного для клиентов.

Форма **set** этой команды используется для указания адреса сервера времени, доступного для клиентов.

Форма **delete** этой команды используется для удаления настройки сервера времени.

Форма **show** этой команды используется для просмотра настройки сервера времени.

35.3.27 service dhcp-server subnet <подсеть_ipv4> wins-server <адрес>

Указание адреса сервера WINS, доступного для клиентов DHCP.

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> wins-server <адрес>
delete service dhcp-server subnet <подсеть_ipv4> wins-server <адрес>
show service dhcp-server subnet <подсеть_ipv4> wins-server
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dhcp-server {
      subnet подсеть_ipv4 {
         wins-server адрес
      }
   }
}
```

Параметры

подсеть_ipv4

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

адрес

Необязательный параметр. Множественный узел. IPv4-адрес сервера WINS NetBIOS, доступного для клиентов DHCP в данной подсети. Сервер WINS предоставляет службы разрешения имен, которые могут использоваться клиентами DHCP Microsoft для соотнесения имен узлов с IP-адресами. Можно указать более одного сервера WINS, выдав эту команду несколько раз.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания адреса сервера WINS, доступного для клиентов DHCP.

Форма **set** этой команды используется для указания адреса сервера WINS, доступного клиентам DHCP.

Форма **delete** этой команды используется для удаления настройки wins-server.

Форма **show** этой команды используется для просмотра настройки wins-server.

35.3.28 service dhcp-server subnet <подсеть_ipv4> wpad-url <адрес>

Указание URL-адреса службы авто-определения веб-прокси (WPAD)

Синтаксис

```
set service dhcp-server subnet <подсеть_ipv4> wpad-url <адрес>
delete service dhcp-server subnet <подсеть_ipv4> wpad-url
show service dhcp-server subnet <подсеть_ipv4> wpad-url
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dhcp-server {
      subnet подсеть_ipv4 {
         wpad-url текст
      }
   }
}
```

Параметры

подсеть_ipv4

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Формат – ipv4-адрес/префикс.

адрес

Необязательный параметр. Указание URL-адреса службы авто-определения веб-прокси (WPAD)

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания URL-адреса службы авто-определения веб-прокси (WPAD).

Форма **set** этой команды используется для указания URL-адреса службы авто-определения веб-прокси (WPAD).

Форма **delete** используется для удаления настройки URL-адреса службы WPAD.

Форма **show** этой команды используется для просмотра настройки URL-адреса службы WPAD.

35.3.29 service dhcp-relay <ip_клиентского_интерфейса>

Синтаксис

```
set service dhcp-relay <ip_клиентского_интерфейса>
delete service dhcp-relay
show service dhcp-relay
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dhcp-relay {
      <ip_клиентского_интерфейса>
   }
```

```
}
```

Параметры

ip_клиентского_интерфейса

Обязательный. Множественный узел. IPv4 или IPv6 адрес, настроенный в системе на каком-либо интерфейсе, который используется в качестве адреса отправителя для ретрансляции пакета на DHCP сервер.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для настройки системы Numa Edge в качестве агента ретрансляции DHCP.

Агент ретрансляции DHCP получает запросы от клиентов DHCP и передает их серверу DHCP. Это позволяет разместить сервер и клиентов DHCP в различных подсетях. Агент ретрансляции перехватывает широковещательное сообщение, отправленное клиентом. На интерфейсе настроен тот же адрес, что и указан в значении параметра ip_клиентского_интерфейса ,то сервер ретрансляции DHCP перенаправляет запрос на DHCP сервер, добавляя указанный адрес в поле GIADDR пакета DHCP. Отправка сообщения происходит по unicast, где в качестве адреса отправителя используется значение параметра *ip_клиентского_интерфейса*, а в качестве адреса получателя – значение параметра server-address.Сервер возвращает ответ агенту ретрансляции, после чего агент транслирует его клиенту с помощью широковещательной рассылки.

ПРИМЕЧАНИЕ В том случае если система одновременно настроена и как сервер DHCP и как агент ретрансляции DHCP, сервер DHCP не будет отвечать запросы клиентов, полученные на интерфейсе, задействованном при ретрансляции в качестве интерфейса клиента (указанного при настройке агента ретрансляции при помощи команды **service dhcp-relay <ip_клиентского_интерфейса>**).
При отключении ретрансляции DHCP запросы клиентов будут обработаны настроенным сервером DHCP.

Форма **set** этой команды используется для настройки системы в качестве агента ретрансляции DHCP.

Форма **delete** этой команды используется для удаления настройки и отключения ретрансляции DHCP.

Форма **show** этой команды используется для просмотра настройки агента ретрансляции DHCP.

35.3.30 service dhcp-relay <ip_клиентского_интерфейса> server-interface <интерфейс>

Указание интерфейса, на котором будут ожидаться ответы от сервера DHCP.

Синтаксис

```
set service dhcp-relay <ip_клиентского_интерфейса> server-interface
<интерфейс>
delete service dhcp-relay <ip_клиентского_интерфейса> server-interface
show service dhcp-relay <ip_клиентского_интерфейса> server-interface
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dhcp-relay {
      ip_клиентского_интерфейса {
         server-interface интерфейс
      }
   }
}
```

Параметры

интерфейс

Идентификатор интерфейса, на котором агент ретрансляции будет ожидать ответы от сервера.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать интерфейс, на котором будут ожидаться ответы от сервера DHCP. Это действие в большинстве случаев не является обязательным. По умолчанию, ответ от сервера DHCP будет обработан на любом интерфейсе. Данная опция позволяетконкретизировать интерфейс, с которого следует получать ответы сервера DHCP. В конфигурации с наличием трёх или более интерфейсов, с наличием подключений к недоверенным сетям эта опция позволяет исключить возможность поддельных ответов через другие интерфейсы.

Настройка отправки запросов к серверу DHCP выполняется через указание IP-адреса сервера DHCP с помощью команды **set service dhcp-relay <ip_клиентского_интерфейса> server-address**.

Форма **set** этой команды используется для указания интерфейса.

Форма **delete** этой команды используется для удаления настройки интерфейса.

Форма **show** этой команды используется для просмотра настройки.

35.3.31 service dhcp-relay <ip_клиентского_интерфейса> server-address <адрес>

Указание IP-адреса сервера DHCP, которому будут передаваться запросы от клиентов DHCP.

Синтаксис

```
set service dhcp-relay <ip_клиентского_интерфейса> server-address <адрес>
delete service dhcp-relay <ip_клиентского_интерфейса> server-address
show service dhcp-relay <ip_клиентского_интерфейса> server-address
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    dhcp-relay {
        ip_клиентского_интерфейса {
            server-address адрес
        }
    }
}
```

Параметры

адрес

Обязательный. IPv4-адрес или IPv6-адрес сервера DHCP, которому будут перенаправляться запросы от клиентов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать адрес сервера DHCP, которому будут передаваться запросы от клиентов DHCP.

Форма **set** этой команды используется для указания адреса сервера DHCP.

Форма **delete** этой команды используется для удаления настройки адреса.

Форма **show** этой команды используется для просмотра настройки.

35.3.32 service dhcp-relay <ip_клиентского_интерфейса> active <состояние>

Возможность отключения ретрансляции DHCP с сохранением настройки.

Синтаксис

```
set service dhcp-relay <ip_клиентского_интерфейса> active <состояние>
delete service dhcp-relay <ip_клиентского_интерфейса> active
show service dhcp-relay <ip_клиентского_интерфейса> active
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dhcp-relay {
      ip_клиентского_интерфейса {
         active состояние
      }
   }
}
```

Параметры

состояние

Формат – on/off. Административное состояние агента ретрансляции DHCP. Допустимые значения:

on: Включение ретрансляции DHCP.

off: Отключение ретрансляции DHCP с сохранением настройки.

Значение по умолчанию

По умолчанию установлено значение on.

Указания по использованию

Данная команда позволяет отключить ретрансляцию DHCP без удаления настройки.

ПРИМЕЧАНИЕ В том случае если система одновременно настроена и как сервер DHCP и как агент ретрансляции DHCP, сервер DHCP не будет отвечать запросы клиентов, полученные на интерфейсе, задействованном при ретрансляциив качестве интерфейса клиента (указанного при настройке агента ретрансляции при помощи команды **service dhcp-relay <ip_клиентского_интерфейса>**). При отключении ретрансляции DHCP запросы клиентовбудут обработаны настроенным сервером DHCP.

Форма **set** этой команды позволяет указать состояние агента ретрансляции DHCP.

Форма **delete** этой команды используется для удаления настройки и восстановления значения, принятого по умолчанию.

Форма **show** этой команды используется для просмотра состояния агента ретрансляции DHCP.

35.3.33 service dhcp-client release interface <интерфейс>

Освобождение текущей клиентской аренды DHCP на интерфейсе.

Синтаксис

```
service dhcp release interface <интерфейс>
```

Режим ввода команды

Эксплуатационный режим.

Параметры

интерфейс

Интерфейс, сконфигурированный на использование DHCP для получения IP-адреса.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для освобождения клиентской аренды DHCP на указанном интерфейсе. Интерфейс должен быть настроен в качестве клиента DHCP и иметь актуальную аренду от сервера.

35.3.34 service dhcp-client renew interface <интерфейс>

Обновление текущей клиентской аренды DHCP на интерфейсе.

Синтаксис

```
service dhcp renew interface <интерфейс>
```

Режим ввода команды

Эксплуатационный режим.

Параметры

интерфейс

Интерфейс, сконфигурированный на использование DHCP для получения IP-адреса.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для обновления клиентской аренды DHCP на указанном интерфейсе. Интерфейс должен быть настроен в качестве клиента DHCP и иметь актуальную аренду от сервера.

35.3.35 service dhcp-client show leases

Отображение сведений DHCP для интерфейсов, настроенных как клиенты DHCP.

Синтаксис

```
show dhcp client leases [interface <интерфейс>]
```

Режим ввода команды

Эксплуатационный режим.

Параметры

интерфейс

Интерфейс, для которого выводятся клиентские сведения.

Указания по использованию

Эта команда используется для просмотра текущих клиентских сведений DHCP для интерфейсов, настроенных в качестве клиентов DHCP.

При использовании без параметра эта команда отображает клиентские сведения со всех интерфейсов, настроенных в качестве клиентов DHCP. Когда в качестве параметра используется интерфейс, команда отображает клиентские сведения с указанного интерфейса.

Для настройки интерфейса в качестве клиента DHCP следует воспользоваться документацией по соответствующему типу интерфейсов.

Примеры

В примере 321 приведен образец вывода команды show dhcp client leases с указанием интерфейса eth2.

Пример 321 - Вывод команды "show dhcp client leases interface eth2"

```
admin@edge:~$ show dhcp client leases interface eth2
interface  : eth2
ip address : 192.168.10.185     [Active]
subnet mask: 255.255.255.0
router     : 192.168.10.254
name server: 8.8.8.8 8.8.4.4
dhcp server: 192.168.10.254
lease time : 600
last update: Thu Oct 8 13:43:29 MSK 2019
```

35.3.36 service dhcp-server show leases

Отображение информации о выделенных адресах DHCP сервером.

Синтаксис

```
show dhcp leases
```

Режим ввода команды

Эксплуатационный режим.

Параметры

Отсутствуют.

Указания по использованию

Эта команда используется для просмотра сведений о текущих арендах для клиентов DHCP.

DHCP настраивается с помощью команды **service dhcp-server**.

Примеры

В примере 322 приведен образец вывода команды show dhcp leases без параметров.

Пример 322- Вывод команды " show dhcp leases"

```
admin@edge:~$ show dhcp leases
 IP address       Hardware Address    Lease expiration          Subnet
Client Name
 ----------       ----------------    ----------------          ---------
-----------
192.168.200.106   00:22:64:53:52:66   Mon Oct 11 14:41:57 2019  default
```

36 DNS

В разделе приведена информация по использованию системы доменных имен Numa Edge, примеры настроек и описание команд, используемых при работе с данной функцией.

- Основная настройка DNS
- Команды настройки DNS

36.1 Настройка службы DNS

В этом разделе рассматриваются следующие вопросы:

- Обзор DNS;
- Примеры настройки DNS.

36.1.1 Обзор DNS

Система доменных имен (DNS) — это распределённая база данных, предоставляющая сопоставления между понятными людям доменными именами и числовыми IP-адресами. Сопоставления DNS фиксируются в ресурсных записях, хранящихся на серверах имен, разбросанных по Интернету. Устройство, которому нужно получить доступ к узлу через Интернет, отправляет запрос DNS на сервер имен. Сервер имен читает свои ресурсные записи и возвращает ответ с IP-адресом указанного имени.

Система DNS формирует свою собственную сеть в Интернете. Если запрошенная запись не является локальной для сервера имен, на который сделан запрос, сервер имен делает запрос на вышестоящий сервер имен и т.д. до тех пор, пока запрошенные сведения не будут найдены и возвращены.

В системе DNS содержатся миллиарды ресурсных записей. Для поддержания управляемости данных записи разделяются на зоны, содержащие ресурсные записи для домена или поддомена DNS.

Система EDGE поддерживает три основные функции, относящиеся к DNS:

- системная DNS;
- динамическая DNS;
- ретрансляция DNS.

Системная DNS

В системной DNS пользователь определяет список серверов имен, которые система Numa Edge может использовать для разрешения имен узлов в IP-адреса. Этот список задается при помощи команды system dns name-server. (пример системной DNS дан в текущем разделе под заголовком «Пример 323 - Настройка статического доступа к серверу имен DNS».)

Динамическая DNS

Изначально сопоставления DNS были статически определены в “файлах зон”, которые периодически загружались на серверы DNS. Такая схема работала приемлемо в те времена, когда большинство узлов были настроены со статическими IP-адресами. Однако начиная с 1990-х годов многим оконечным точкам сетей IP-адреса присваиваются с помощью динамических протоколов, таких как протокол DHCP. До 1997 года устройства с IP-адресами, назначенными с помощью DHCP, в принципе не могли участвовать в системе DNS.

В 1997 году группа IETF (Internet Engineering Task Force) опубликовала предложение RFC 2136 «*Динамические обновления в системе доменных имен*», в котором описывался протокол динамического обновления DNS. Динамическая DNS (DDNS) обеспечивает механизм динамической установки и удаления записей DNS. Устройства, использующие динамическую DNS, могут в реальном времени извещать сервер доменных имен об изменениях в имени узла, IP-адресе или других сведениях, имеющих отношение к DNS.

Эта функция особенно полезна для систем, которым динамический адрес выделяется поставщиком услуг доступа к Интернету (провайдером Интернета). Если IP-адрес меняется, система Numa Edge извещает поставщика службы DDNS об изменении. Поставщик службы DDNS несет ответственность за распространение изменения на другие серверы DNS. Система Numa Edge поддерживает несколько поставщиков службы DDNS.

Ретрансляция DNS

Во многих средах, где используются подключения провайдеров Интернета для конечных пользователей, провайдер назначает клиентскому маршрутизатору IP-адрес и извещает его о сервере DNS, который следует использовать. Во многих случаях IP-адрес самого сервера DNS назначается через DHCP и периодически меняется; провайдер извещает клиентский маршрутизатор об изменении IP-адреса сервера DNS с помощью периодических обновлений. Это делает проблематичной статическую настройку IP-адреса сервера DNS на сервере DHCP клиентского маршрутизатора для клиентов в его локальной сети.

В подобных случаях для поддержания связи между узлами в локальной сети и сервером DNS провайдера Интернета в системе Numa Edge может использоваться ретрансляция DNS.

Когда используется ретрансляция DNS, клиентский маршрутизатор предлагает в качестве адреса сервера DNS для узлов в своей сети свой собственный адрес (который является статическим), так что все клиентские запросы DNS делаются к адресу клиентской стороны маршрутизатора. Получив запрос DNS, клиентский маршрутизатор ретранслирует его серверу DNS провайдера Интернета; ответы от него направляются назад на маршрутизатор и ретранслируются через него на клиентские узлы. Если провайдер Интернета изменяет адрес своего сервера DNS, клиентский маршрутизатор просто переписывает его адрес внутри себя. С точки зрения клиентов в локальной сети адрес сервера остается неизменным.

Другим преимуществом ретрансляции DNS является то обстоятельство, что запросы DNS кэшируются в системе Numa Edge (либо до истечения времени жизни, настроенного в записи DNS, либо до заполнения кэша). Ответы на последующие запросы к кэшированному элементу даются локально, что приводит к соответствующему сокращению трафика глобальной сети и уменьшению времени ответа для клиентов.

36.1.2 Примеры настройки DNS

В этом разделе рассматриваются следующие вопросы:

- Настройка доступа к серверу имен;
- Настройка динамического DNS;
- Настройка ретрансляции DNS;
- Статически настроенные записи и ретрансляция DNS.

В этом разделе есть следующие примеры:

- Пример 323 - Настройка статического доступа к серверу имен DNS
- Пример 324 - Настройка динамической DNS
- Пример 325 - Настройка ретрансляции DNS
- Пример 326 - Настройка статических записей

Настройка доступа к серверу имен

Для получения возможности перевода имен узлов (например, www.numatech.ru) в IP-адреса (например, 203.0.113.67) система должна иметь возможность доступа к серверу DNS.

В примере 323 выполняется настройка статического IP-адреса для сервера DNS с адресом 203.0.113.78. Для соответствующей настройки системы Numa Edge выполните следующие действия.

Пример 323 - Настройка статического доступа к серверу имен DNS

Действие	Команда
Указание IP-адреса сервера DNS.	`[edit]` `admin@edge# set system dns name-server 203.0.113.78`

Настройка динамической DNS

На рисунке ниже показана типичная картина DDNS. В этой картине:

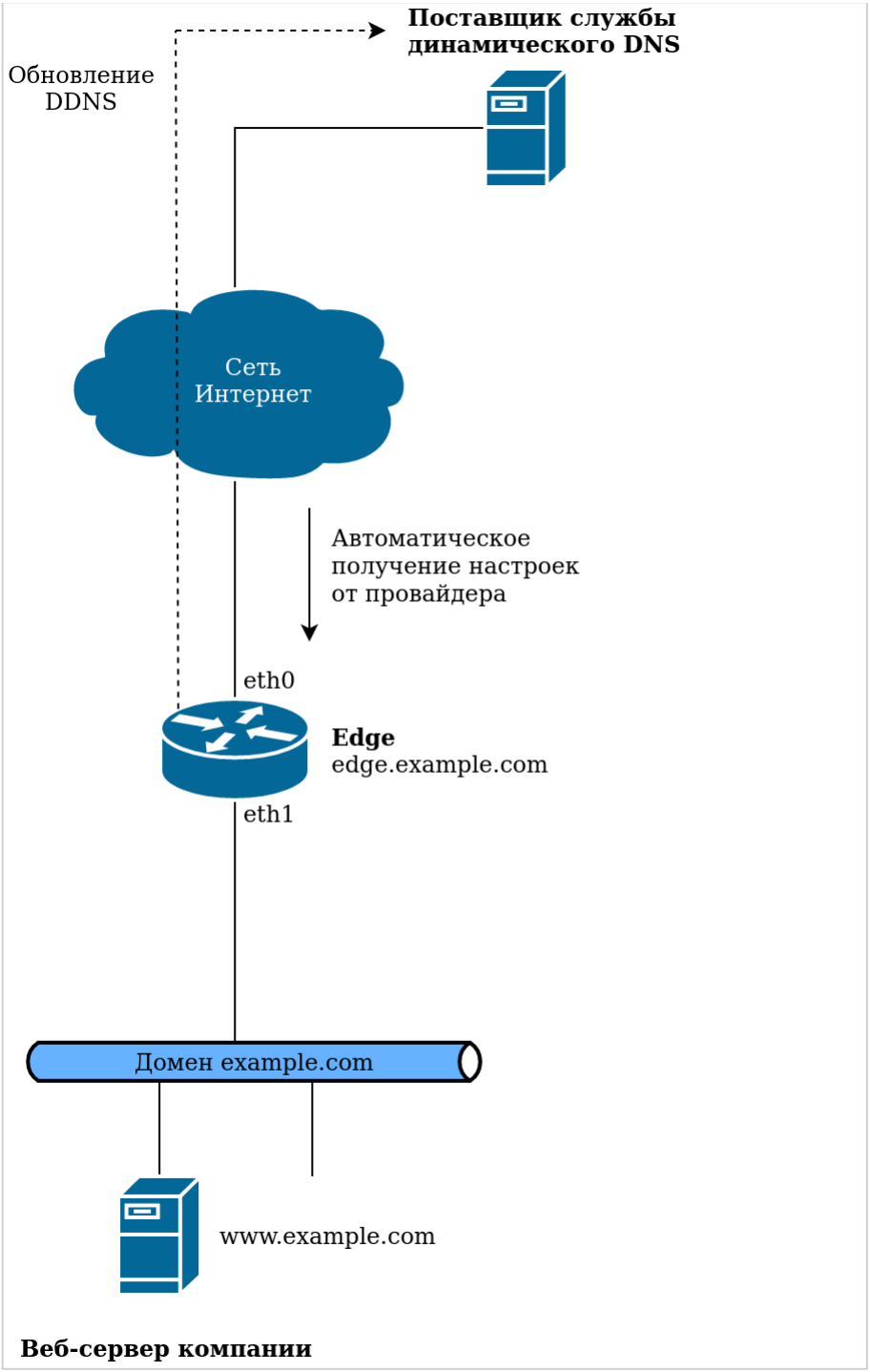


Рис. 1 - Схема работы DDNS

- Edge подключен к интернет-провайдеру через интерфейс eth0;
- Сетевой домен - **com**;
- Имя узла системы Numa Edge - **edge.example.com**;
- Веб-сервер компании расположен за системой EDGE. Имя его узла **www.example.com**;
- Интернет-провайдер предоставляет своим клиентам динамические IP-адреса с помощью DHCP;
- IP-адрес интерфейса eth0 системы Numa Edge время от времени меняется вследствие динамического назначения интернет-провайдером;
- Веб-сервер компании расположен за устройством с преобразованием сетевых адресов (NAT) под управлением системы Numa Edge, так что его IP-адрес (как он видится из Интернета) изменяется, когда интернет-провайдер назначает новый адрес интерфейсу eth0;
- Так как адрес веб-сервера меняется, ответы на запросы к DNS на разрешение имени **www.example** также должны меняться, отражая новый IP-адрес. DDNS решает эту проблему.

DDNS позволяет Numa Edge обновлять сведения об IP-адресах для любых локальных имен узлов (например, **edge.example.com** и **www.example.com**) в системе DNS, если IP-адрес на интерфейсе eth0 изменяется. Процедура настройки выглядит следующим образом:

1. Подписка на подключение к службе DDNS от одного из поддерживаемых поставщиков службы:

- DNSPark
- DSL Reports: www.dslreports.com;
- DynDNS: www.dyndns.com;
- EasyDNS: www.easydns.com;
- namecheap: www.namecheap.com;
- SiteSolutions: www.sitelutions.com;
- zoneedit: www.zoneedit.com.

Указания по подключению доступны у поставщиков служб.

2. Настройка системы Numa Edge согласно сведениям, предоставленным поставщиком службы, таким как имя службы, идентификатор входа и пароль, чтобы система могла подключиться к службе и отправлять обновления поставщику службы DDNS.

3. Настройка списка имен узлов, требующих обновления записей в системе DNS при изменении IP-адреса на интерфейсе eth0, в Numa Edge.

ПРИМЕЧАНИЕ В зависимости от поставщика службы, включение имени домена в имя узла может требоваться или нет (например, “www” вместо “www.example.com”).

В примере 324 выполняется настройка DDNS для поставщика службы EasyDNS. В примере предполагается, что подписка на услуги DynDNS уже имеется). Для соответствующей настройки системы Numa Edge выполните следующие действия в режиме настройки.

Пример 324 - Настройка динамической DNS

Действие	**Команда**
Настройка поставщика DDNS.	`[edit]` `admin@edge# set service dns dynamic interface eth0 service easydns`
Установка идентификатора входа для поставщика DDNS (например, dnsuser).	`[edit]` `admin@edge# set service dns dynamic interface eth0 service easydns login dnsuser`
Установка пароля для поставщика DDNS (например, dnspassword).	`[edit]` `admin@edge# set service dns dynamic interface eth0 service easydns password dnspassword`
Указание edge в качестве имени узла, запись DNS которого нуждается в обновлении при изменении IP-адреса на интерфейсе eth0.	`[edit]` `admin@edge# set service dns dynamic interface eth0 service easydns host-name edge.example.com`
Указание www в качестве имени узла, запись DNS которого нуждается в обновлении при изменении IP-адреса на интерфейсе eth0.	`[edit]` `admin@edge# set service dns dynamic interface eth0 service easydns host-name www.example.com`
Фиксация изменения.	`[edit]` `admin@edge# commit`

Вывод настройки динамического DNS.	`[edit]`
	`admin@edge# show service dns dynamic`
	`  interface eth0 {`
	`  service easydns {`
	`  host-name edge.example.com`
	`  host-name www.example.com`
	`  login dnsuser`

Действие	Команда
	password dnspassword } }

Теперь, если IP-адрес интерфейса eth0 изменится, Numa Edge автоматически подключится к службе EasyDNS с идентификатором входа **dnsuser** и паролем **dnspassword**. Она отправит обновления для имен узлов **edge.example.com** и **www.example.com**, в которых будет указан новый IP-адрес, требуемый для доступа к этим узлам в домене **example.com**. Внешние пользователи, запрашивающие DNS для разрешения имен **edge.example.com** или **www.example.com**, получат от системы DNS ответ с новым адресом.

Настройка ретрансляции DNS

Настройка EDGE для ретрансляции DNS состоит из двух основных этапов:

1. Указание DNS-серверов , на которые следует передавать запросы
2. Указание интерфейсов, на которых будет выполняться прослушивание запросов DNS

1. Указание DNS-серверов

Местонахождение серверов имен можно получить из трех мест:

- Из системного списка DNS-серверов, определенного при помощи команды **set system dns name-server**.
- По DHCP.
- Из перечня добавочных DNS-серверов установленных при помощи команды **set service dns forwarding listen-on address**.

По умолчанию система направляет DNS-запросы на DNS-сервера из системного списка серверов имен, а также из списка DNS-серверов, полученного через DHCP. Поведение по умолчанию можно переопределить, указав как минимум один из приведенных ниже пунктов.

- Использовать только системные DNS-сервера. Для этого используется команда системы **set service dns forwarding**.
- Использовать дополнительные DNS-сервера, определённые при помощи команды **set service dns forwarding listen-on address**.

При запуске или перезапуске службы ретрансляции DNS она отправляет сообщения всем DNS-серверам в пуле и выбирает первый ответивший DNS-сервер. Этот сервер используется до тех пор, пока он не станет недоступным, в этом случае система отправляет новое сообщение оставшимся DNS-серверам в пуле.

Местонахождение DNS-серверов можно указать с помощью команды **set service dns forwarding listen-on address**. Можно указать более одного адреса, использовав эту команду несколько раз.

2. Указание прослушиваемых интерфейсов

Прослушиваемые интерфейсы – это интерфейсы, на которые внутренние клиенты будут посылать DNS-запросы. Служба ретрансляции DNS получает эти сообщения и передает на DNS-сервер.

Для установки прослушиваемого интерфейса используется команда **set service dns forwarding listen-on interface**. Можно указать более одного интерфейса, использовав эту команду несколько раз.

После выполнения вышеуказанных действий служба ретрансляция DNS будет настроена. Теперь можно настроить DHCP-сервер для распространения прослушивающегося адреса ретрансляции DNS клиентам DHCP. (Сведения о настройке сервера DHCP в системе Numa Edge приведены в разделе DHCP).

На рисунке ниже показана типичная схема применения ретрансляции DNS. На этой схеме:

- Интернет-провайдер своим клиентам, в том числе системе Numa Edge динамические IP-адреса по DHCP;
- Numa Edge обеспечивает службу DHCP для клиентов в своей локальной сети;
- Локальные клиенты отправляют DNS-запросы устройству Numa Edge;
- Служба ретрансляции DNS на устройстве Numa Edge передает запросы на DNS-сервер Интернет-провайдера.

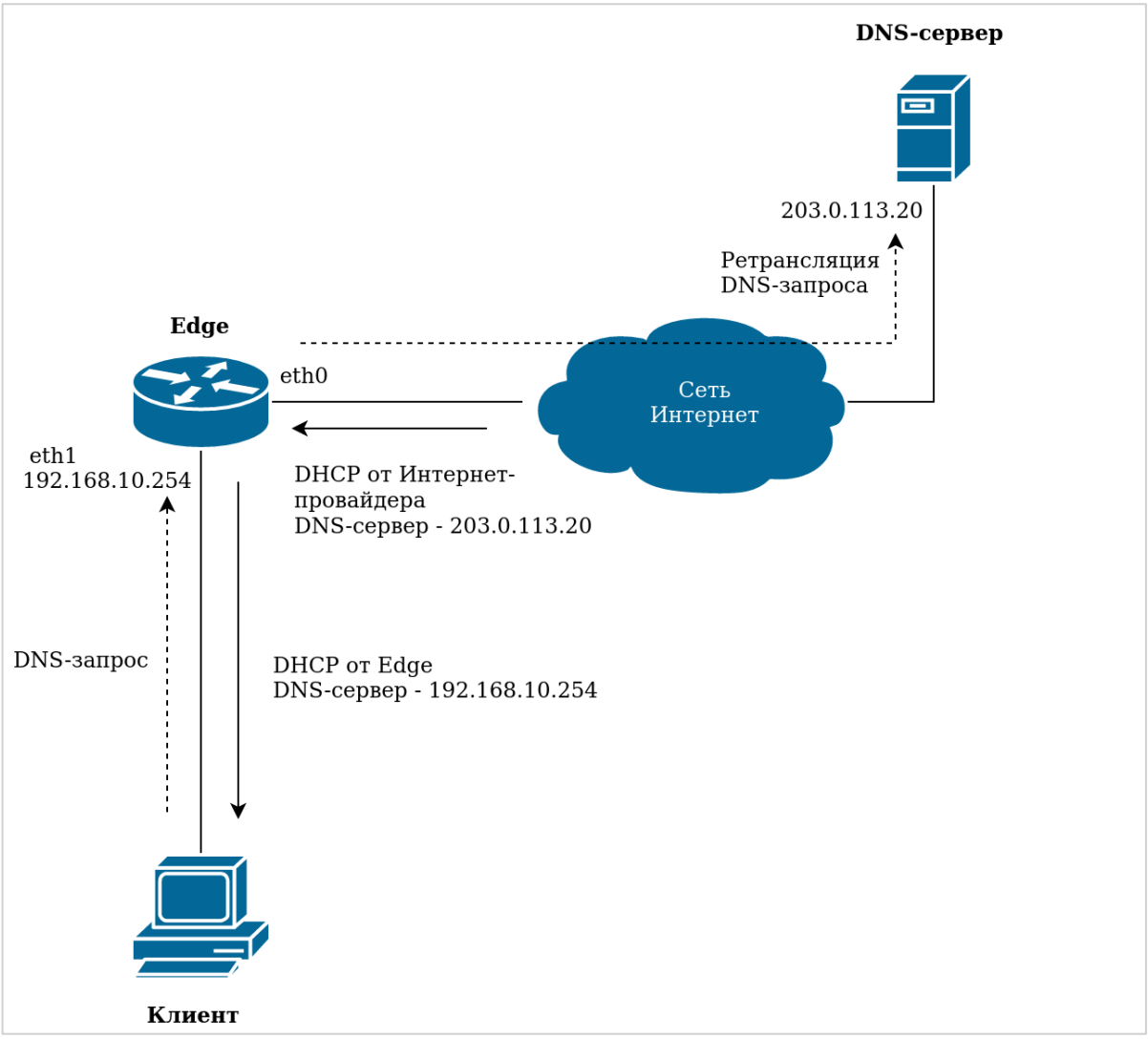


Рисунок 83 – Схема работы ретрансляции DNS-запросов

В примере 325 выполняется настройка ключевых компонентов Numa Edge для описанной выше схемы. Для соответствующей настройки системы Numa Edge выполните следующие действия в режиме настройки.

Пример 325 - Настройка ретрансляции DNS

Действие	**Команда**
Настройка IP-адреса и префикса на eth1	`[edit]` `admin@edge# set interfaces ethernet eth1 address 192.168.10.254/24`
Установка eth0 в качестве клиента DHCP	`[edit]` `admin@edge# set interfaces ethernet eth0 address dhcp`
Установка сервера DHCP на EDGE путем создания узла конфигурации для подсети 192.168.10.0/24. Ввод начального и конечного IP-адресов для пула.	`[edit]` `admin@edge# set service dhcp-server subnet 192.168.10.0/24 start 192.168.10.100 stop 192.168.10.199`
Указание маршрутизатора по умолчанию для клиентов DHCP подсети 192.168.10.0/24.	`[edit]` `admin@edge# set service dhcp-server subnet 192.168.10.0/24 default-router 192.168.10.254`
Указание списка DNS-серверов с использованием сведений о DNS-серверах, предоставляемых DHCP-сервером провайдера (на eth0).	`[edit]` `admin@edge# set service dns forwarding listen-on address 192.168.10.254`
Прослушивание DNS-запросов на eth1	`[edit]`

Действие	Команда
	admin@edge# set service dns forwarding listen-on interface eth1
Указание DNS-сервера для DHCP-клиентов (в этом случае устройство будет работать как ретранслятор DNS в сети 192.168.10.0/24).	[edit] admin@edge# set service dhcp-server subnet 192.168.10.0/24 dns-server 192.168.10.254
Фиксация изменения.	[edit] admin@edge# commit

Вывод настройки, относящейся к DNS.	[edit]
	admin@edge# show service dns
	forwarding {
	listen-on {
	address 192.168.10.254
	interface eth1
	}
	}

Статические записи и ретрансляция DNS

В связи со сложностью взаимодействия с преобразованием сетевых адресов (NAT) в корпоративном шлюзе возможны проблемы с получением корректных IP-адресов в корпоративной сети. Для обхода этой проблемы (а также для использования в других ситуациях) существует возможность создать статические записи локально на Numa Edge при помощи команды **system static-host-mapping**. Любые записи, созданные подобным образом, используются при обработке входящих DNS-запросов ещё до передачи запросов на ретрансляцию. Если соответствие находится, возвращается соответствующий IP-адрес.

В примере 326 выполняется настройка системы на возвращение IP-адреса 203.0.113.78 при получении запроса DNS на “example.com” либо «vhost1».

Пример 326 - Настройка статических записей

Действие	Команда
Создание узла конфигурации для статического сопоставления узла.	[edit] admin@edge# set system static-host-mapping host-name example.com
Ввод псевдонима для узла (не обязательно).	[edit] admin@edge# set system static-host-mapping host-name example.com alias vhost1
Указание IP-адреса для возвращения в ответ на запрос к DNS.	[edit] admin@edge# set system static-host-mapping host-name example.com inet 203.0.113.78
Фиксация изменения.	[edit] admin@edge# commit

Вывод настройки статического сопоставления узлов.	[edit]
	admin@edge# show system static-host-mapping
	host-name example.com{
	alias vhost1
	inet 203.0.113.78
	}

36.2 Команды службы DNS

Команды настройки динамической DNS:

Команда настройки	
service dns dynamic interface <интерфейс>	Включение поддержки DDNS на интерфейсе.
service dns dynamic interface <интерфейс> active <состояние>	Возможность отключения DDNS на интерфейсе с сохранением настройки.
service dns dynamic interface <интерфейс> service <сервис>	Указание поставщика службы DDNS.

service dns dynamic interface <интерфейс> service <сервис> host-name <имя_узла>	Указание имени узла, для которого требуется обновление записи DNS у поставщика службы DDNS.
service dns dynamic interface <интерфейс> service <сервис> login <имя_входа_на_сервис>	Ввод идентификатора входа для аутентификации у поставщика службы DDNS.
service dns dynamic interface <интерфейс> service <сервис> password <пароль_сервиса>	Ввод пароля для аутентификации у поставщика службы DDNS.
service dns dynamic interface <интерфейс> service <сервис> server <адрес>	Указание сервера, на который следует отправлять обновления DDNS.
Команды настройки ретрансляции DNS	
service dns forwarding listen-on interface <интрефейс>	Указание имени интерфейса, на котором будут прослушиваться запросы DNS.
service dns forwarding listen-on address <адрес>	Указание адреса интерфейса, на котором будут прослушиваться запросы DNS.
Эксплуатационные команды	
service dns clear forwarding all	Очистка всех связанных с DNS счетчиков и кэша ретрансляции DNS.
service dns clear forwarding cache	Удаление всех записей из кэша ретрансляции DNS.
service dns show dynamic status	Отображение состояния обновления для всех узлов, настроенных для обновления динамической DNS
service dns show forwarding nameservers	Отображение серверов имен, используемых для ретрансляции DNS.
service dns show forwarding statistics	Отображение счетчиков, имеющих отношение к ретрансляции DNS.
service dns update dynamic interface <интерфейс>	Отправка принудительного обновления поставщику службы DDNS на указанном интерфейсе.

36.2.1 service dns dynamic interface <интерфейс>

Включение поддержки DDNS на интерфейсе.

Синтаксис

```
set service dns dynamic interface <интерфейс>
delete service dns dynamic interface <интерфейс>
show service dns dynamic interface [<интерфейс>]
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    dns {
        dynamic {
            interface интерфейс {
            }
        }
    }
}
```

Параметры

интерфейс

Множественный узел. Интерфейс, который должен поддерживать DDNS.

Можно включить поддержу DDNS более чем на одном интерфейсе путем создания нескольких узлов конфигурации interface.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания интерфейсов, которые будут поддерживать динамический DNS (DDNS).

Форма **set** этой команды используется для включения DDNS на интерфейсе.

Форма **delete** этой команды используется для отключения DDNS на интерфейсе и удаления всей настройки DDNS.

Форма **show** этой команды используется для просмотра настройки DDNS.

36.2.2 service dns dynamic interface <интерфейс> active <состояние>

Возможность отключения сервиса DDNS на интерфейсе с сохранением настройки.

Синтаксис

```
set service dns dynamic interface <интерфейс> active <состояние>
delete service dns dynamic interface <интерфейс> active
show service dns dynamic interface <интерфейс> active
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    dns {
        dynamic {
            interface интерфейс {
                active состояние
            }
        }
    }
}
```

Параметры

интерфейс

Множественный узел. Интерфейс, поддерживающий DDNS.

состояние

Административное состояние сервиса DDNS для указанного интерфейса. Поддерживаются следующие значения:

on: Включение сервиса DDNS.

off: Отключение сервиса DDNS без отбрасывания настройки.

Значение по умолчанию

Сервис DDNS включен.

Указания по использованию

Эта команда используется для указания состояния сервиса DDNS на интерфейсе с сохранением настройки.

Форма **set** этой команды используется для указания состояния сервиса DDNS на указанном интерфейсе.

Форма **delete** этой команды используется для удаления настройки и восстановления значения по умолчанию.

Форма **show** этой команды используется для просмотра состояния сервиса DDNS.

36.2.3 service dns dynamic interface <интерфейс> service <сервис>

Указание поставщика службы DDNS.

Синтаксис

```
set service dns dynamic interface <интерфейс> service <сервис>
delete service dns dynamic interface <интерфейс> service <сервис>
show service dns dynamic interface <интерфейс> service
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    dns {
        dynamic {
            interface интерфейс {
                service сервис {
                }
            }
        }
    }
}
```

Параметры

интерфейс

Множественный узел. Интерфейс, поддерживающий DDNS.

сервис

Множественный узел. Имя поставщика сервиса DDNS. Поддерживаются следующие значения: dnspark, dslreports, dyndns, easydns, namecheap, sitelutions и zoneedit. Можно указать более одного поставщика DDNS на интерфейс путем создания нескольких узлов конфигурации service.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания организаций, поставляющих сервисы динамического DNS (DDNS) для системы EDGE.

Форма **set** этой команды используется для указания поставщика сервиса DDNS.

Форма **delete** этой команды используется для удаления поставщика сервиса DDNS из настройки.

Форма **show** этой команды используется для просмотра сведений о поставщике сервиса DDNS.

36.2.4 service dns dynamic interface <интерфейс> service <сервис> host-name <имя_узла>

Указание имени узла, для которого требуется обновление записи DNS у поставщика сервиса DDNS.

Синтаксис

```
set service dns dynamic interface <интерфейс> service <сервис> host-name
<имя_узла>
delete service dns dynamic interface <интерфейс> service <сервис> host-name
<имя_узла>
```

```
show service dns dynamic interface <интерфейс> service <сервис> host-name
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    dns {
        dynamic {
            interface интерфейс {
                service сервис {
                    host-name имя_узла
                }
            }
        }
    }
}
```

Параметры

интерфейс

Множественный узел. Интерфейс, поддерживающий DDNS.

сервис

Множественный узел. Имя поставщика сервиса DDNS. Поддерживаются следующие значения: dnspark, dslreports, dyndns, easydns, namecheap, sitelutions и zoneedit.

имя_узла

Имя узла, для которого требуется обновление записи DNS у поставщика службы DDNS.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания имени узла, для которого требуется обновление записи DNS у поставщика сервиса DDNS.

Форма **set** этой команды используется для указания имени узла.

Форма **delete** этой команды используется для удаления имени узла из настройки.

Форма **show** этой команды используется для просмотра настройки имени узла.

36.2.5 service dns dynamic interface <интерфейс> service <сервис> login <имя_входа_на_сервис>

Ввод идентификатора входа для аутентификации у поставщика сервиса DDNS.

Синтаксис

```
set service dns dynamic interface <интерфейс> service <сервис> login
<имя_входа_на_сервис>
delete service dns dynamic interface <интерфейс> service <сервис> login
show service dns dynamic interface <интерфейс> service <сервис> login
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dns {
      dynamic {
         interface интерфейс {
            service сервис {
               login имя_входа_на_сервис
            }
         }
      }
   }
}
```

Параметры

интерфейс

Множественный узел. Интерфейс, поддерживающий DDNS.

сервис

Множественный узел. Имя поставщика сервиса DDNS. Поддерживаются следующие значения: dnspark, dslreports, dyndns, easydns, namecheap, sitelutions и zoneedit.

имя_входа_на_сервис

Идентификатор входа, который используется при входе на сервис поставщика DDNS.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания идентификатора входа, который система должна использовать при входе на сервис поставщика DDNS.

Форма **set** этой команды используется для указания идентификатора входа, который система должна использовать при входе на сервис поставщика DDNS.

Форма **delete** этой команды используется для удаления идентификатора ввода для поставщика DDNS.

Форма **show** этой команды используется для просмотра настройки идентификатора входа для поставщика DDNS.

36.2.6 service dns dynamic interface <интерфейс> service <сервис> password <пароль_сервиса>

Ввод пароля для аутентификации у поставщика DDNS.

Синтаксис

```
set service dns dynamic interface <интерфейс> service <сервис> password <пароль_сервиса>
delete service dns dynamic interface <интерфейс> service <сервис> password
show service dns dynamic interface <интерфейс> service <сервис> password
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dns {
```

```
        dynamic {
            interface интерфейс {
                service сервис {
                    password пароль_сервиса
                }
            }
        }
    }
}
```

Параметры

интерфейс

Множественный узел. Интерфейс, поддерживающий DDNS.

сервис

Множественный узел. Имя поставщика DDNS. Поддерживаются следующие значения: dnspark, dslreports, dyndns, easydns, namecheap, sitelutions и zoneedit.

пароль_службы

Пароль для использования системой при входе в систему поставщика DDNS.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания пароля, который система должна использовать при входе на систему поставщика DDNS.

Форма **set** этой команды используется для указания пароля для поставщика DDNS.

Форма **delete** этой команды используется для удаления пароля поставщика DDNS.

Форма **show** этой команды используется для просмотра настройки пароля поставщика DDNS.

36.2.7 service dns dynamic interface <интерфейс> service <сервис> server <адрес>

Указание сервера, на который следует отправлять обновления DDNS.

Синтаксис

```
set service dns dynamic interface <интерфейс> service <сервис> server <адрес>
delete service dns dynamic interface <интерфейс> service <сервис> server
show service dns dynamic interface <интерфейс> service <сервис> server
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    dns {
        dynamic {
            interface интерфейс {
                service сервис {
                    server адрес
                }
            }
```

```
        }
    }
}
```

Параметры

интерфейс

Множественный узел. Интерфейс, поддерживающий DDNS.

сервис

Множественный узел. Имя поставщика сервиса DDNS. Поддерживаются следующие значения: dnspark, dslreports, dyndns, easydns, namecheap, sitelutions и zoneedit.

адрес

IP-адрес или имя узла сервера поставщика сервиса DDNS, на который следует отправлять обновления DDNS. Требуется не для всех поставщиков сервиса DDNS.

Значение по умолчанию

Используются серверы по умолчанию поставщика сервиса DDNS.

Указания по использованию

Эта команда используется для указания IP-адреса или имени узла сервера поставщика сервиса DDNS, на который следует отправлять обновления DDNS. Установка сервера требуется только в том случае, если он специфицируется поставщиком сервиса DDNS.

Форма **set** этой команды используется для указания сервера, на который следует отправлять обновления DDNS.

Форма **delete** этой команды используется для возврата к использованию серверов по умолчанию поставщика сервиса DDNS.

Форма **show** этой команды используется для просмотра настройки серверов поставщика сервиса DDNS.

36.2.8 service dns forwarding listen-on interface <интрефейс>

Указание имени интерфейса, на котором будут прослушиваться запросы DNS.

Синтаксис

```
set service dns forwarding listen-on interface <интрефейс>
delete service dns forwarding listen-on interface <интрефейс>
show service dns forwarding listen-on interface
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
    dns {
        forwarding {
            listen-on interface интрефейс
        }
    }
}
```

Параметры

интерфейс

Множественный узел. Интерфейс, на котором следует прослушивать клиентские запросы DNS.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания интерфейса, на котором будут прослушиваться клиентские запросы DNS. Интерфейс должен быть заранее настроен в системе. Для работы ретрансляции DNS нужно указать как минимум один IP-адрес или интерфейс. Можно указать более одного интерфейса для приема клиентских запросов DNS путем создания нескольких узлов конфигурации listen-on interface.

Форма **set** этой команды используется для указания интерфейса, на котором следует прослушивать запросы DNS.

Форма **delete** этой команды используется для прекращения прослушивания запросов DNS на интерфейсе.

Форма **show** этой команды используется для просмотра настройки прослушивания запросов DNS.

36.2.9 service dns forwarding listen-on address <адрес>

Указание адреса интерфейса, на котором будут прослушиваться запросы DNS.

Синтаксис

```
set service dns forwarding listen-on address <адрес>
delete service dns forwarding listen-on address <адрес>
show service dns forwarding listen-on address
```

Режим ввода команды

Режим настройки.

Ветвь конфигурации

```
service {
   dns {
      forwarding {
         listen-on address адрес
      }
   }
}
```

Параметры

адрес

Множественный узел. IP-адрес, на котором следует прослушивать клиентские запросы DNS. IP-адрес должен быть сконфигурирован заранее на каком-либо из интерфейсов системы.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания IP-адреса, на котором будут прослушиваться клиентские запросы DNS. Адрес должен быть заранее настроен в системе. Для работы ретрансляции DNS нужно указать как минимум один IP-адрес или интерфейс. Можно указать более одного IP-адреса для приема клиентских запросов DNS путем создания нескольких узлов конфигурации listen-on address.

Форма **set** этой команды используется для указания интерфейса, на котором следует прослушивать запросы DNS.

Форма **delete** этой команды используется для прекращения прослушивания запросов DNS на интерфейсе.

Форма **show** этой команды используется для просмотра настройки прослушивания запросов DNS.

36.2.10 service dns clear forwarding all

Очистка всех связанных с DNS счетчиков и кэша ретрансляции DNS.

Синтаксис

```
service dns clear forwarding all
```

Режим ввода команды

Эксплуатационный режим.

Параметры

Отсутствует.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для очистки всех счетчиков, связанных с ретрансляцией DNS. Все записи в кэше ретрансляции DNS удаляются.

36.2.11 service dns clear forwarding cache

Удаление всех записей из кэша ретрансляции DNS.

Синтаксис

```
service dns clear forwarding cache
```

Режим ввода команды

Эксплуатационный режим.

Параметры

Отсутствует.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для удаления всех записей в кэше ретрансляции DNS.

36.2.12 service dns show dynamic status

Отображение состояния обновления для всех узлов, настроенных для обновления динамической DNS.

Синтаксис

```
service dns show dynamic status
```

Режим ввода команды

Эксплуатационный режим.

Параметры

Отсутствует

Указания по использованию

Эта команда используется для отображения состояния обновления для всех имен узлов, настроенных для обновления с помощью динамическим DNS (DDNS).

Примеры

В примере 327 показан образец вывода команды **service dns show dynamic status**.

Пример 327 - Вывод сведений для узлов, настроенных для DDNS

```
admin@edge:~$ service dns show dynamic status
show dns dynamic status
interface     : eth0
ip address    : 203.0.113.97
host-name     : serv1.example.com
last update   : Thu Mar 20 08:45:06 2020
update-status: good

interface     : eth0
ip address    : 203.0.113.98
host-name     : serv2.example.com
last update   : Thu Mar 20 08:45:06 2020
update-status: good
```

36.2.13 service dns show forwarding nameservers

Отображение DNS-серверов, используемых для ретрансляции DNS.

Синтаксис

```
service dns show forwarding nameservers
```

Режим ввода команды

Эксплуатационный режим.

Параметры

Отсутствует

Указания по использованию

Эта команда используется для отображения DNS-серверов , которые в текущий момент используются для ретрансляции DNS, а также DNS-серверов, которые доступны, но в настоящий момент для ретрансляции DNS не используются.

Примеры

В примере 328 показан образец вывода команды **service dns show forwarding nameservers**.

Пример 328 - Вывод сведений о серверах имен, касающихся ретрансляции DNS

```
admin@edge:~$ service dns show forwarding nameservers
----------------------
Nameservers configured for DNS forwarding
----------------------
203.0.113.80 available via 'system'

----------------------
Nameservers NOT configured for DNS forwarding
----------------------
203.0.113.81 available via 'dhcp eth0'
```

36.2.14 service dns show forwarding statistics

Отображение счетчиков, имеющих отношение к ретрансляции DNS.

Синтаксис

```
service dns show forwarding statistics
```

Режим ввода команды

Эксплуатационный режим.

Параметры

Отсутствует

Указания по использованию

Эта команда используется для вывода статистических сведений, относящихся к ретрансляции DNS. Подсчет статистики перезапускается каждый раз, когда происходит изменение DNS-серверов, полученных из любого источника (по DHCP, из системы или настроенных статически), изменение в статическом сопоставлении узлов (выполненное по команде system static-host-mapping) или изменение в настройке ретрансляции DNS.

Примеры

В примере 329 показан образец вывода команды **service dns show forwarding statistics**.

Пример 329 - Отображение статистики ретрансляции DNS

```
admin@edge:~$ service dns show forwarding statistics
--------
Cache statistics
--------
Cache size: 74
Queries forwarded: 3
Queries answered locally: 1
Total DNS entries inserted into cache: 15
DNS entries removed from cache before expiry: 0

-----------
Nameserver statistics
-----------
Server: 203.0.113.80
Queries sent: 3
Queries retried or failed: 0
```

36.2.15 service dns update dynamic interface <интерфейс>

Отправка принудительного обновления поставщику службы DDNS на указанном интерфейсе.

Синтаксис

```
service dns update dynamic interface <интерфейс>
```

Режим ввода команды

Эксплуатационный режим.

Параметры

интерфейс

Интерфейс, с которого следует отправить принудительное обновление.

Указания по использованию

Эта команда используется для принудительной отправки вручную обновления поставщику сервиса динамического DNS (DDNS). Принудительное обновление предоставляет поставщику сервиса DDNS сведения о текущем состоянии указанного интерфейса.

ПРИМЕЧАНИЕ Обратите внимание, что частые ненужные обновления могут вызвать блокировку имени узла поставщиком сервиса DDNS, поэтому эту команду не следует использовать регулярно.

37 SNMP

37.1 Обзор SNMP

SNMP (Simple Network Management Protocol)— это протокол управления сетями связи на основе архитектуры UDP. Основной концепцией протокола является то, что вся необходимая для управления устройством информация хранится на самом устройстве в так называемой базе управляющей информации (MIB – Management Information Base). MIB представляет собой набор переменных (OID), характеризующих состояние объекта управления. Эти OID имеют цифровой формат в виде иерахрической древовидной структуры, представленной на рисунке ниже.

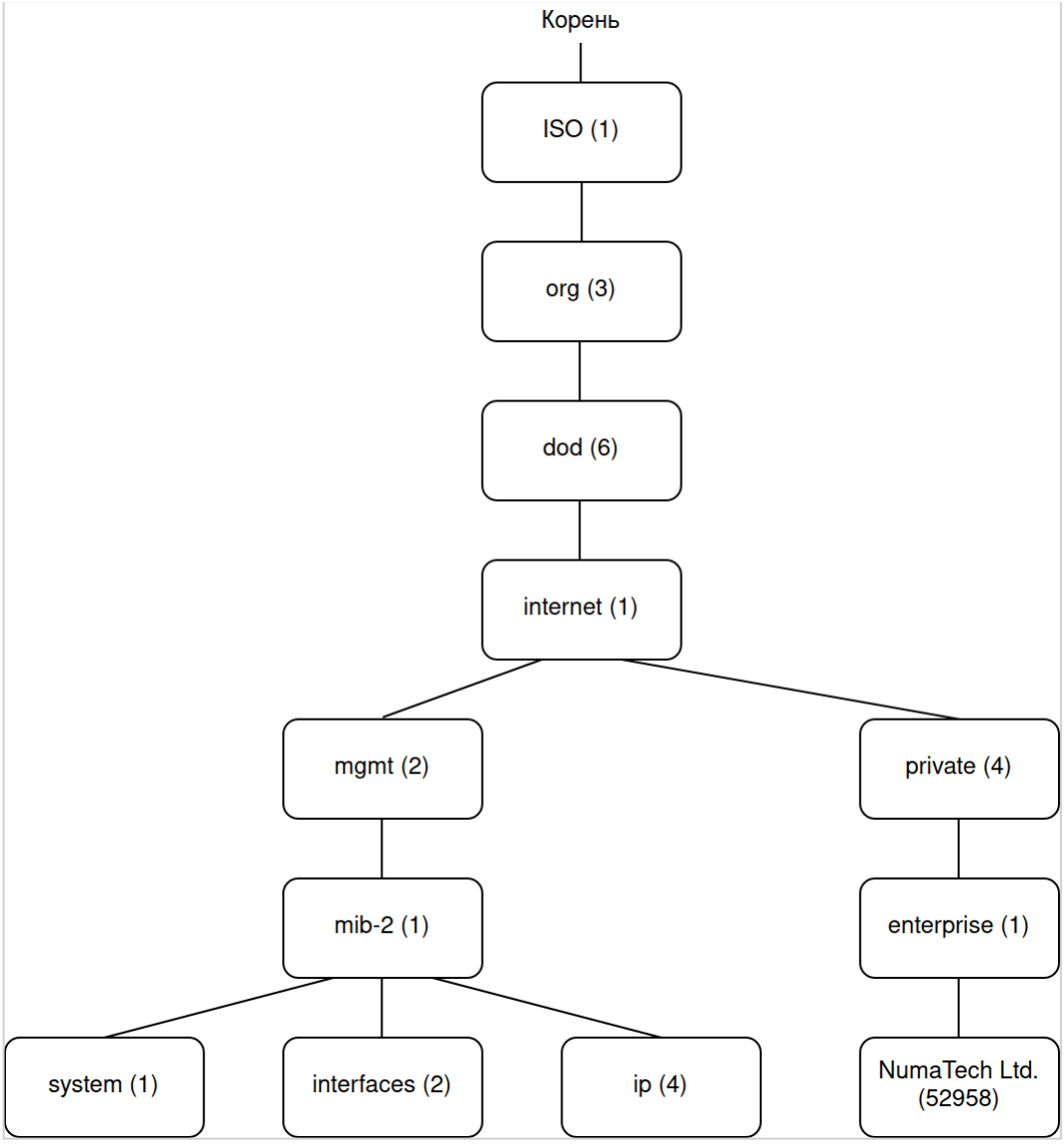


Рисунок 84- Схема OID для протокола SNMP.

На данной схеме представлена сама специфика построения OID для определенного MIB. Список поддерживаемых MIB.

Пример получения одного из OID для имени системы Numa Edge (объект sysName).

Таблица 272 - Представление OID в виде таблицы

iso	International Organization for Standardization (ISO)
identified-organization	Схема определения организации согласно ISO/IEC 6523-2
dod	United States Department of Defense (DoD). Эта организация изначально занималась стандартизацией протокола
internet	Интернет

mgmt	IETF Management
mib-2	База OID для спецификации MIB-2
system	Характеристики системы
sysName	Имя системы

В Numa Edge поддерживаются следующие стандартные базы управляющей информации:

Таблица 273- Поддерживаемые стандартные базы управляющей информации

Название MIB	**OID**	**Документ**	**Примечание**
BGP4-MIB	1.3.6.1.2.1.15	RFC 1657, Definitions of Managed Objects for the Fourth Version of Border Gateway Protocol (BGP-4)	Поддерживаются уведомительные сообщения при переходе BGP FSM в состояние Established (bgpEstablished trap), при переходе с состояния с меньшим номером (bgpBackwardTransition trap).
DISMAN-EVENT-MIB	1.3.6.1.2.1.88	RFC 2571,Event MIB	
ENTITY-MIB	1.3.6.1.2.1.47	RFC 4133, Entity MIB (Version 3)	
HOST-RESOURCES-MIB	1.3.6.1.2.1.25	RFC 2790, Host Resources MIB	
IF-MIB	1.3.6.1.2.1.2	RFC 2863, The Interfaces Group MIB	Поддерживаются уведомительные сообщения при разрыве / восстановлении соединения (linkUp, linkDown traps).
IP-MIB	1.3.6.1.2.1.4	RFC 2011, SNMPv2 Management Information Base for the Internet Protocol using SMIv2	
IP-FORWARD-MIB	1.3.6.1.2.1.4.24	RFC 4292, IP Forwarding Table MIB	
IPV6-MIB	1.3.6.1.2.1.55	RFC2465, Management Information Base for IP Version 6: Textual Conventions and General Group	
OSPF-MIB	1.3.6.1.2.1.14	RFC 1850, OSPF Version 2 Management Information Base	
NOTIFICATION-LOG-MIB	1.3.6.1.2.1.92	RFC 3014, Notification Log MIB	
RFC1213-MIB	1.3.6.1.2.1	RFC 1213, Management Information Base for Network Management of TCP/IP-based internets: MIB-II	
RIPv2-MIB	1.3.6.1.2.1.23	RFC 1724, RIP Version 2 MIB Extension	
SNMPv2-MIB	1.3.6.1.2.1.1	RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)	Поддерживаются уведомительные сообщения при холодном / горячем старте (coldStart, warmStart traps).
TCP-MIB	1.3.6.1.2.1.6	RFC 4022, Management Information Base for the Transmission Control Protocol (TCP)	

Название MIB	OID	Документ	Примечание
UDP-MIB	1.3.6.1.2.1.7	RFC 4113, Management Information Base forthe User Datagram Protocol (UDP)	

SNMP как сетевой протокол предоставляет только набор команд для работы с переменными MIB. Этот набор включает следующие операции:

- get-request - используется для запроса одного или более параметров MIB.
- get-next-request - используется для последовательного чтения значений. Обычно используется для чтения значений из таблиц. После запроса первой строки при помощи get-request get-next-request используют для чтения оставшихся строк таблицы.
- set-request - используется для установки значения одной или более переменных MIB.
- get-response - возвращает ответ на запрос get-request, get-next-request или set-request.
- trap - уведомительное сообщение о событиях типа холодного или горячего запуска, или обрыве соединения.

В основе взаимодействий лежит клиент-серверная модель. Роль сервера выполняет компонент управляемой системы, называемый агентом, который отвечает на запросы управляющей системы, называемой также менеджером SNMP.

Помимо ответов на запросы управляющей системы агент SNMP может формировать и отправлять уведомительные сообщения о событиях. Агент асинхронно отправляет уведомления управляющей системе, указанной в качестве получателя таких сообщений при помощи команды service snmp trap-target <адрес>.

В Numa Edge по умолчанию определены следующие идентификаторы объектов:

- sysObjectID= NET-SNMP-MIB::netSnmpAgentOIDs.10 , где значение 10 - соответствует идентификатору SNMP агента linux.
- sysDescr = Numa Edge

Значение для sysDescr может быть изменено при помощи команды service snmp description <описание>.

37.1.1 Примеры настройки SNMP

В этом разделе рассматриваются следующие вопросы:

- определение сообщества SNMP;
- указание параметров получателя уведомительных сообщений о событиях.

В данных примерах определяется сообщество SNMP, включающее 3 узла, которые выступают в роли менеджеров SNMP. Numa Edge настраивается таким образом, чтобы отправлять уведомительные сообщения (trap) всем этим менеджерам SNMP. После выполнения всех настроек, Numa Edge будет настроен в соответствии с рисунком ниже.

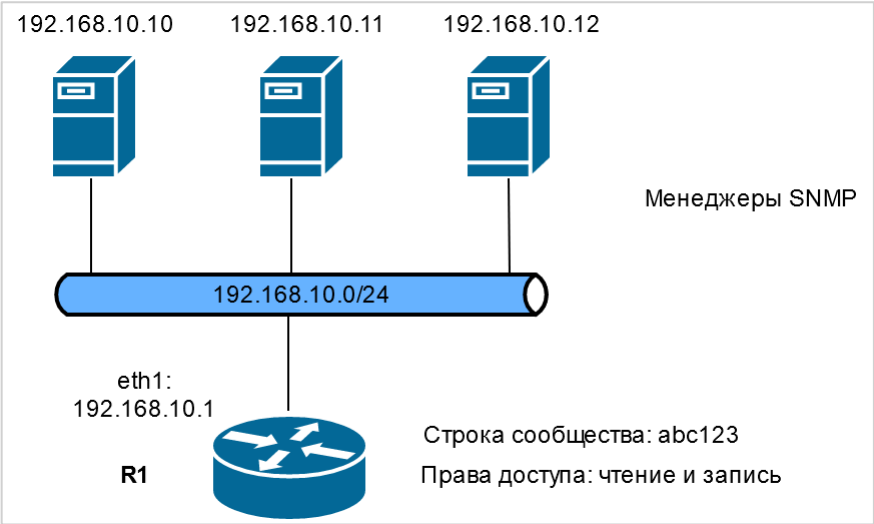


Рисунок 85 – Настройка SNMP

В этом разделе есть следующие примеры:

- Пример 330 - Определение сообщества SNMP
- Пример 331- Указание параметров получателей уведомительных сообщений о событияхОпределение сообщества SNMP

Сообщество SNMP представляет собой список клиентов SNMP, авторизованных для отправки запросов к данной системе. Авторизация происходит на основе строки сообщества. Строка сообщества представляет собой пароль, обеспечивающий защиту от нелегитимных запросов SNMP.

- в том случае если не указано ни одного клиента, тогда любой клиент, предоставляющий правильную строку сообщества, сможет получить доступ на чтение;
- в том случае если определен хотя бы один клиент или сеть, то только указанные клиенты и/или сети смогут получить доступ к данной системе. Права доступа для клиентов определяются параметром authorization. (По умолчанию установлены права только на чтение.)

В примере 330 в качестве строки сообщества SNMP указывается abc123, а также определяются 3 клиента для данного сообщества: 192.168.10.10, 192.168.10.11 и 192.168.10.12. Для данного сообщества устанавливается доступ на чтение и на запись.

Для указания параметров сообщества SNMP необходимо выполнить следующие шаги в режиме настройки:

Пример 330 - Определение сообщества SNMP

Действие	**Команда**
Создание узлов конфигурации snmp и community. Указание строки сообщества.	`[edit]` `admin@edge# set service snmp community abc123`

Указание списка клиентов SNMP для данного сообщества.	`[edit]`
	`admin@edge# set service snmp community abc123 client 192.168.10.10`
	`[edit]`
	`admin@edge# set service snmp community abc123 client 192.168.10.11`
	`[edit]`
	`admin@edge# set service snmp community abc123 client 192.168.10.12`

Для данного сообщества устанавливается доступ на чтение и на запись.	`[edit]` `admin@edge# set service snmp community abc123 authorization rw`
Фиксация изменений	`[edit]` `admin@edge# commit`

- Указание параметров получателя уведомительных сообщений о событиях

В примере 331 определяются параметры получателей для уведомительных сообщений о событиях: 192.168.10.10, 192.168.10.11 и 192.168.10.12.

Для указания параметров получателей уведомительных сообщений SNMP необходимо выполнить следующие шаги в режиме настройки:

Пример 331- Указание параметров получателей уведомительных сообщений о событиях

Действие	**Команда**

Указание получателей.	`[edit]`
	`admin@edge# set service snmp trap-target 192.168.10.10`
	`[edit]`
	`admin@edge# set service snmp trap-target 192.168.10.11`
	`[edit]`
	`admin@edge# set service snmp trap-target 192.168.10.12`

Фиксация изменений.	`[edit]` `admin@edge# commit`

37.2 Команды SNMP

Команды настройки	
service snmp	Указание параметров SNMP.
service snmp active <состояние>	Возможность отключения сервиса SNMP с сохранением настройки.
service snmp community <сообщество>	Указание сообщества SNMP.
service snmp community <сообщество> authorization <доступ>	Указание прав доступа, которыми будет обладать указанное сообщество.
service snmp community <сообщество> client <адрес>	Указание клиентов SNMP для данного сообщества, которые могут иметь доступ к системе.
service snmp community <сообщество> network <подсеть>	Указание сети клиентов SNMP для данного сообщества, которые могут получить доступ к системе.
service snmp contact <контактная_инф>	Указание контактной информации для системы.
service snmp description <описание>	Указание краткого описания.
service snmp listen-address <адрес>	Указание IP-адреса, который будет прослушиваться агентом SNMP на предмет входящих запросов.
service snmp location <местоположение>	Указание местоположения.
service snmp trap-source <адрес>	Указание IP-адреса источника для уведомительных сообщений о событиях (SNMP traps).
service snmp trap-target <адрес>	Указание адреса назначения для уведомительных сообщений о событиях SNMP (traps).
Эксплуатационные команды	
show snmp	Отображение сведений для SNMP.

37.2.1 service snmp

Указание параметров SNMP.

Синтаксис

```
set service snmp
delete service snmp
show service snmp
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
```

```
    snmp {
    }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для настройки сведений о сообществах SNMP, позволяет указать местоположение и контактную информацию, а также адрес назначения для отправки уведомлений о событиях (traps).

Форма **set** данной команды используется для определения настроек SNMP.

Форма **delete** данной команды используется для удаления конфигурации SNMP.

Форма **show** данной команды используется для отображения конфигурации SNMP.

37.2.2 service snmp active <состояние>

Возможность отключения сервиса SNMP с сохранением настройки.

Синтаксис

```
set service snmp active <состояние>
delete service snmp active
show service snmp active
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    snmp {
        active состояние
    }
}
```

Параметры

состояние

Административное состояние сервиса SNMP. Поддерживаются следующие значения:

on: Включение сервиса SNMP.

off: Отключение сервиса SNMP без отбрасывания настройки.

Значение по умолчанию

Сервис SNMP включен.

Указания по использованию

Эта команда используется для отключения сервиса SNMP с сохранением настройки.

Форма **set** данной команды используется для указания состояния сервиса SNMP.

Форма **delete** данной команды используется для восстановления значения по умолчанию.

Форма **show** данной команды используется для отображения состояния сервиса SNMP.

37.2.3 service snmp community <сообщество>

Указание сообщества SNMP.

Синтаксис

```
set service snmp community <сообщество>
delete service snmp community <сообщество>
show service snmp community <сообщество>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    snmp {
        community сообщество
    }
}
```

Параметры

сообщество

Необязательный. Множественный узел. Указание сообщества SNMP. Значение данного параметра определяет строку сообщества, которая используется для авторизации менеджеров SNMP, отправляющих запросы Numa Edge. Допустимо использование букв, цифр, а также дефиса. Для того чтобы определить несколько сообществ, необходимо создать соответствующее количество узлов конфигурации community.

Значение по умолчанию

По умолчанию не определено ни одного сообщества.

Указания по использованию

Данная команда позволяет определить сообщество SNMP.

Форма **set** данной команды используется для указания сообщества SNMP.

Форма **delete** данной команды используется для удаления указанного сообщества SNMP.

Форма **show** данной команды используется для отображения конфигурации сообществ SNMP.

37.2.4 service snmp community <сообщество> authorization <доступ>

Указание прав доступа, которыми будет обладать указанное сообщество.

Синтаксис

```
set service snmp community <сообщество> authorization <доступ>
delete service snmp community <сообщество> authorization
show service snmp community <сообщество> authorization
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    snmp {
        community сообщество {
            authorization доступ
        }
    }
```

```
}
```

Параметры

сообщество

Необязательный. Множественный узел. Указание сообщества SNMP. Значение данного параметра определяет строку сообщества, которая используется для авторизации менеджеров SNMP, отправляющих запросы Numa Edge. Допустимо использование букв, цифр, а также дефиса. Для того чтобы определить несколько сообществ, необходимо создать соответствующее количество узлов конфигурации community.

доступ

Формат – ro/rw. Необязательный. Указание прав доступа, которыми будет обладать указанное сообщество. Поддерживаемые значения:

ro: Данное сообщество будет иметь доступ только на чтение информации и не сможет изменять ее.

rw: Данное сообщество будет иметь доступ на чтение и запись.

Удаление узла конфигурации authorization приводит к восстановлению значения, принятого по умолчанию (ro).

Значение по умолчнию

По умолчанию установлено значение ro.

Указания по использованию

Данная команда позволяет указать права доступа для сообщества SNMP.

Форма **set** данной команды используется для установки прав доступа для сообщества SNMP.

Форма **delete** данной команды используется для восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения конфигурации прав доступа для сообщества SNMP.

37.2.5 service snmp community <сообщество> client <адрес>

Указание клиентов SNMP для данного сообщества, которые могут иметь доступ к системе.

Синтаксис

```
set service snmp community <сообщество> client <адрес>
delete service snmp community <сообщество> client <адрес>
show service snmp community <сообщество> client
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   snmp {
      community сообщество {
         client адрес
      }
   }
}
```

Параметры

сообщество

Необязательный. Множественный узел. Указание сообщества SNMP. Значение данного параметра определяет строку сообщества, которая используется для авторизации менеджеров SNMP, отправляющих запросы Numa Edge. Допустимо использование букв, цифр, а также дефиса. Для того чтобы определить несколько сообществ, необходимо создать соответствующее количество узлов конфигурации community.

адрес

Необязательный. Множественный узел. Клиенты SNMP, которые могут иметь доступ к данной системе. Формат представляет собой IPv4 и IPv6 адреса.

Для того чтобы определить несколько клиентов, необходимо создать соответствующее количество узлов конфигурации client.

В том случае если не указано ни одного клиента, тогда любой клиент, предоставляющий правильную строку сообщества сможет получить доступ на чтение. В том случае если определен хотя бы один клиент или сеть, то только указанные клиенты и/или сети смогут получить доступ к данной системе.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать клиентов SNMP для данного сообщества, которые смогут получить доступ к системе.

Форма **set** данной команды используется для указания клиентов SNMP для данного сообщества, которые смогут получить доступ к системе.

Форма **delete** данной команды используется для удаления из конфигурации клиентов SNMP.

Форма **show** данной команды используется для отображения конфигурации клиентов SNMP.

37.2.6 service snmp community <сообщество> network <подсеть>

Указание сети клиентов SNMP для данного сообщества, которые могут получить доступ к системе.

Синтаксис

```
set service snmp community <сообщество> network <подсеть>
delete service snmp community <сообщество> network <подсеть>
show service snmp community <сообщество> network
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   snmp {
      community сообщество {
         network подсеть
      }
   }
}
```

Параметры

сообщество

Необязательный. Множественный узел. Указание сообщества SNMP. Значение данного параметра определяет строку сообщества, которая используется для авторизации менеджеров SNMP, отправляющих запросы Numa edge. Допустимо использование букв, цифр, а также дефиса. Для того чтобы определить несколько сообществ, необходимо создать соответствующее количество узлов конфигурации community.

подсеть

Необязательный. Множественный узел. Сеть клиентов SNMP для данного сообщества, которые могут получить доступ к системе. Формат – ipv4-адрес/префикс|ipv6-адрес/префикс. Для того чтобы определить несколько сетей, необходимо создать соответствующее количество узлов конфигурации network.

В том случае если не указано ни одного клиента, тогда любой клиент, предоставляющий правильную строку сообщества сможет получить доступ на чтение. В том случае если определен хотя бы один клиент или сеть, то только указанные клиенты и/или сети смогут получить доступ к данной системе.

Значение по умолчанию

Отсутствуют.

Указания по использованию

Данная команда позволяет указать сеть клиентов SNMP, которые могут получить доступ к системе.

Форма **set** данной команды позволяет указать сеть клиентов SNMP, которые могут получить доступ к системе.

Форма **delete** данной команды позволяет удалить конфигурацию сети клиентов SNMP.

Форма **show** данной команды позволяет отобразить конфигурацию сети клиентов SNMP для данного сообщества.

37.2.7 service snmp contact <контактная_инф>

Указание контактной информации для системы.

Синтаксис

```
set service snmp contact <контакт_инф>
delete service snmp contact
show service snmp contact
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   snmp {
      contact контактн_инф
   }
}
```

Параметры

контактн_инф

Необязательный. Указание контактной информации для системы. Это значение хранится в ветви системной информации MIB-2 (system information) в файле snmpd.conf. Допустимо использование букв, цифр, а также дефиса.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать контактную информацию.

Форма **set** данной команды используется для указания контактной информации.

Форма **delete** данной команды используется для удаления контактной информации.

Форма **show** данной команды используется для отображения контактной информации для данной системы.

37.2.8 service snmp description <описание>

Указание краткого описания.

Синтаксис

```
set service snmp description <описание>
delete service snmp description
```

```
show service snmp description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    snmp {
        description описание
    }
}
```

Параметры

описание

Необязательный. Указание краткого описания. Это значение хранится в ветви системной информации MIB-2 (system information) в файле snmpd.conf. Допустимо использование букв, цифр, а также дефиса.

ПРИМЕЧАНИЕ Данный параметр позволяет установить значение для объекта sysDescr. По умолчанию для sysDescr установлено значение Numa Edge.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания краткого описания для системы.

Форма **set** данной команды используется для указания краткого описания.

Форма **delete** данной команды используется для удаления описания.

Форма **show** данной команды используется для отображения краткого описания

37.2.9 service snmp listen-address <адрес>

Указание IP-адреса, который будет прослушиваться агентом SNMP на предмет входящих запросов.

Синтаксис

```
set service snmp listen-address <адрес> [port <порт>]
delete service snmp listen-address  <адрес> [port]
show service snmp listen-address  <адрес> [port]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    snmp {
        listen-address <адрес> {
            port <порт>
        }
    }
}
```

Параметры

адрес

Необязательный. Множественный узел. Адрес IPv4 или IPv6, на котором агент SNMP будет ожидать запросы.

порт

Прослушиваемый порт UDP. По умолчанию используется порт 161. Значение должно лежать в диапазоне 1-65535.

Значение по умолчанию

Агент SNMP ожидает запросов на всех адресах на сетевом порту 161.

Указания по использованию

Данная команда позволяет указать адрес IPv4 или IPv6, на котором агент SNMP будет ожидать входящие запросы.

Форма **set** данной команды позволяет указать прослушиваемый адрес.

Форма **delete** данной команды используется для удаления конфигурации прослушиваемого адреса и восстановления значения, используемого по умолчанию.

Форма **show** данной команды используется для отображения конфигурации.

37.2.10 service snmp location <местоположение>

Указание местоположения.

Синтаксис

```
set service snmp location <местоположение>
delete service snmp location
show service snmp location
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   snmp {
      location местоположение   }
}
```

Параметры

местоположение

Необязательный. Указание местоположения. Это значение хранится в ветви системной информации MIB-2 (system information) в файле snmpd.conf. Допустимо использование букв, цифр, а также дефиса.

Значение по умолчанию

Отсутствуют.

Указания по использованию

Данная команда позволяет указать местоположение.

Форма **set** данной команды позволяет указать местоположение.

Форма **delete** данной команды используется для удаления местоположения.

Форма **show** данной команды используется для отображения местоположения.

37.2.11 service snmp trap-source <адрес>

Указание IP-адреса источника для уведомительных сообщений о событиях (SNMP traps).

Синтаксис

```
set service snmp trap-source <адрес>
delete service snmp trap-source <адрес>
show service snmp trap-source
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    snmp {
        trap-source адрес
    }
}
```

Параметры

адрес

IPv4 или IPv6-адрес источника уведомительных сообщений SNMP.

Этот адрес будет указан в качестве источника уведомительных сообщений о событиях, отправляемых серверу SNMP. Должен быть указан адрес, настроенный на одном из интерфейсов Numa Edge. По умолчанию автоматически выбирается IP-адрес, настроенный на одном из интерфейсов.

Значение по умолчанию

Адрес источника уведомительных сообщений выбирается автоматически.

Указания по использованию

Данная команда позволяет указать IP-адрес источника уведомительных сообщений о событиях, отправляемых серверу SNMP.

Форма **set** данной команды используется для указания адреса источника.

Форма **delete** используется для удаления адреса источника и восстановления автоматического выбора адреса.

Форма **show** данной команды позволяет отобразить адрес источника уведомительных сообщений.

37.2.12 service snmp trap-target <адрес>

Указание адреса назначения для уведомительных сообщений о событиях SNMP (traps).

Синтаксис

```
set service snmp trap-target <адрес> [community <сообщество> | port <порт>]
delete service snmp trap-target <адрес> [community | port]
show service snmp trap-target <адрес> [community | port]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    snmp {
        trap-target адрес {
            community сообщество
            port порт
        }
    }
}
```

Параметры

адрес

Необязательный. Множественный узел. IPv4 или IPv6-адрес назначения для уведомительных сообщений SNMP. Для того чтобы указать несколько адресов назначения, следует создать соответствующее количество узлов конфигурации trap-target.

сообщество

Имя сообщества, используемое для отправки уведомительных сообщений о событиях. По умолчанию используется сообщество public.

порт

Порт назначения, используемый для уведомительных сообщений. По умолчанию установлено значение 162. Значение должно лежать в диапазоне 1-65535.

Значение по умолчанию

Отсутствуют.

Указания по использованию

Данная команда используется для указания IP-адрес и порта назначения для уведомительных сообщений SNMP, а также используемого имени сообщества.

Форма **set** данной команды используется для указания параметров получателя уведомительных сообщений о событиях.

Форма **delete** данной команды используется для удаления параметров получателя уведомительных сообщений о событиях.

Форма **show** данной команды используется для отображения конфигурации параметров получателя уведомительных сообщений о событиях.

37.2.13 show snmp

Отображение сведений для SNMP.

Синтаксис

```
show snmp
```

Режим ввода команды

Эксплуатационный режим.

Параметры

Отсутствуют.

Указания по использованию

Эта команда используется для отображения состояния SNMP.

38 Балансировка нагрузки

38.1 Обзор функций и примеры настройки

38.1.1 Обзор функции балансировки нагрузки

В данном разделе рассматриваются общие вопросы по использованию функции балансировки нагрузки в системе Numa Edge.

Описание механизма балансировки нагрузки

Numa Edge поддерживает функцию балансировки нагрузки по нескольким каналам как для транзитного (проходящего), так и для локального трафика, используя таблицы маршрутизации. Балансировка нагрузки обеспечивает избыточность по путям на случай неработоспособности маршрутов отдельно взятой таблицы маршрутизации. Описываемая функция является качественным дополнением к функциям политик маршрутизации, в частности она выполняет задачи по динамическому управлению балансировкой нагрузки основываясь на контроле доступности таблиц маршрутизации.

Таблица маршрутизации рассматривается как работоспособная при условии успешного прохождения соответствующих проверок. Для каждой таблицы маршрутизации должен быть сконфигурирован критерий исправности, который включает в себя число неудачных проверок работоспособности, после которого таблица маршрутизации объявляется неработоспособной, и число удачных проверок, необходимых для объявления о восстановлении работоспособности таблицы маршрутизации.

Если для проверки работоспособности настраивается несколько целевых адресов, то администратор получает возможность не полагаться на один целевой узел, который может не отвечать на запросы по причинам, отличным от сбоя пути. Проверка по нескольким целям будет выполняться до тех пор, пока проверка не закончится успешно или список проверок не будет исчерпан. В одном тесте можно указать только один целевой узел. Для того чтобы использовать несколько целевых узлов, необходимо создать соответствующее количество тестов.

Процесс балансировки нагрузки автоматически устанавливает маршруты, настроенные администратором для каждого пути, и осуществляет балансировку трафика в соответствии с работоспособностью путей и весами, примененными к каждой таблице маршрутизации. Пути, установленные в таблицах маршрутизации, можно вывести командой **routing table show <имя_таблицы> route**.

Правила балансировки нагрузки

Балансировка нагрузки настраивается в качестве упорядоченного набора правил, в которых указываются род трафика (определенного фильтром) подлежащего балансировке, набор таблиц маршрутизации и их относительные веса.

Каждое правило содержит набор критериев соответствия и набор таблиц маршрутизации с назначенными весами. Правила балансировки нагрузки нумеруются и исполняются в соответствующем порядке.

Следует учесть, что в настроенном правиле балансировки нагрузки номер является неизменяемым идентификатором. Для изменения номера правила, его следует удалить и создать заново с новым номером.

По этой причине рекомендуется назначать правилам балансировки нагрузки номера, оставляя пустые интервалы. Например, можно создать набор правил балансировки нагрузки с номерами 10, 20, 30 и т.д. Таким образом, в случае необходимости добавления еще одного правила в конкретном месте в текущей последовательности правил, это будет возможно сделать без удаления текущего набора правил.

Для создания или изменения правила балансировки нагрузки используются команды **set** и узел конфигурации **policy route** с указанием имени правила балансировки нагрузки.

Проверка работоспособности таблиц маршрутизации

Таблица маршрутизации, участвующая в балансировке нагрузки, считается активным членом пула до тех пор, пока она проходит проверки работоспособности. Наблюдение за работоспособностью таблицы маршрутизации осуществляется путем отправки сообщений эхо-запроса ICMP («пинга») на удаленную точку назначения через некоторый интервал времени. В случае успешного ответа от точки назначения, таблица маршрутизации признается прошедшей тест на проверку работоспособности. В случае сбоя проверки работоспособности, таблица маршрутизации удаляется из пула активных таблиц маршрутизации.

Также существует проверка на основе времени жизни (ttl), при которой на целевой адрес отправляется пакет UDP с ограничением ttl.

Когда сбойная таблица маршрутизации восстанавливает работоспособность, она вновь добавляется к списку активных членов пула, чтобы система балансировки нагрузки смогла ее использовать. Система определяет работоспособность пути с помощью периодической проверки работоспособности опросом удаленной цели или нескольких целей.

Настройка проверки работоспособности таблиц маршрутизации состоит из следующих элементов:

- Допустимое число сбоев проверок работоспособности, после которых таблица маршрутизации считается неработоспособной. Используется команда **load-balancing table-health <имя_таблицы> failure-count <число>.**
- Определение теста работоспособности таблицы маршрутизации. Используется команда **load-balancing table-health <имя_таблицы> test <номер_теста>.**
- Максимальное время ожидания ответа на сообщение эхо-запроса, которое можно считать удачным выполнением проверки. Используется команда
- **load-balancing table-health <имя_таблицы> test <номер_теста> resp-time <секунды>.**
- Указание целевого узла для проверки работоспособности. Используется команда **load-balancing table-health <имя_таблицы> test <номер_теста> target <адрес>.**
- Указание ограничения числа транзитных участков для теста типа tll. Используется команда **load-balancing table-health <имя_таблицы> test <номер_теста> ttl-limit <ограничение>.**
- Указание типа теста для проверки работоспособности таблицы маршрутизации (**ping**, либо **ttl**). Используется команда **load-balancing table-health <имя_таблицы> test <номер_теста> type <тип>.**
- Установка количества последовательных успешных проверок работоспособности таблицы маршрутизации. Используется команда **load-balancing table-health <имя_таблицы> success-count <число>.**

Этапы настройки балансировки нагрузки

Балансировка нагрузки настраивается в 2 этапа:

1. Настройка политик для обеспечения балансировки нагрузки на интерфейсы через нужную таблицу маршрутизации.
2. Определение цели (или целей), достижимых с каждой таблицы маршрутизации, участвующей в балансировке нагрузки. Цель используется службой проверки работоспособности таблиц маршрутизации для определения доступности проверяемой таблицы.

38.1.2 Примеры настройки

В данном разделе рассматриваются следующие вопросы:

- базовая настройка балансировки нагрузки;
- использование весов в таблицах маршрутизации;
- переход на резервную таблицу маршрутизации при неработоспособности остальных таблиц маршрутизации.

Базовая настройка балансировки нагрузки

В текущем примере описана базовая настройка балансировки нагрузки. Свойства приведенной настройки:

- балансировка всего трафика, входящего на маршрутизатор Edge через интерфейс eth1, и преобразование адресов отправителей (SNAT) осуществляются на интерфейсах eth2 и eth3;
- проверка таблиц маршрутизации Gateway_ISP1 и Gateway_ISP2 на работоспособность осуществляется путем отправки эхо-запросов на удаленные цели (в примере используются следующие удаленные цели: 192.0.2.1, 192.0.2.2, 192.0.2.3 и 192.0.2.4);
- таблица маршрутизации Gateway_ISP1 удаляется из пула активных таблиц маршрутизации после трех последовательных сбоев эхо-запроса, а таблица маршрутизации Gateway_ISP2 — после пяти последовательных сбоев.

Пример базовой настройки балансировки нагрузки приведен на рисунке ниже.

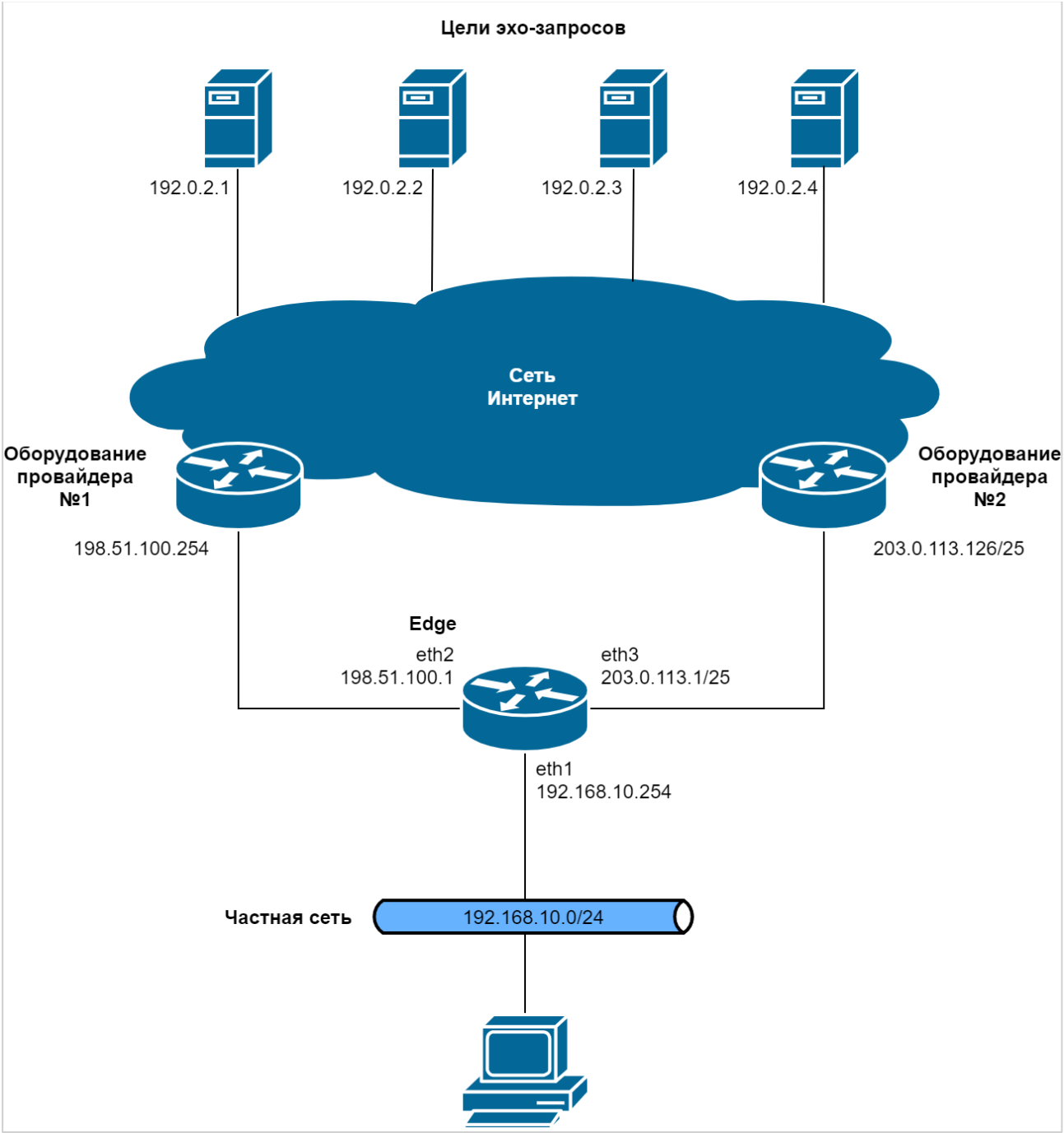


Рисунок 86 – Пример базовой настройки балансировки нагрузки

В примере ниже приведена настройка SNAT, создание политики балансировки нагрузки и маршрутов по умолчанию к двум поставщикам услуг доступа к сети Интернет (198.51.100.254 и 203.0.113.126), между которыми будет выполняться балансировка нагрузки.

Пример 332- Настройка SNAT, создание политики балансировки нагрузки и маршрутов по умолчанию

Действие	**Команда**
Создание правила 10, преобразующего сетевой адрес отправителя (SNAT).	`[edit]` `admin@edge# set service nat ipv4 rule 10 type masquerade`
Применение правила 10 к пакетам, которые были отправлены любым узлом сети 192.168.10.0/24.	`[edit]` `admin@edge# set service nat ipv4 rule 10 source address 192.168.10.0/24`
Применение правила 10 к пакетам, для которых	`[edit]`

Действие	**Команда**
исходящим интерфейсом является `eth2`.	`admin@edge# set service nat ipv4 rule 10 outbound-interface eth2`
Создание правила 20, преобразующего сетевой адрес отправителя (SNAT).	`[edit]` `admin@edge# set service nat ipv4 rule 20 type masquerade`
Применение правила 20 к пакетам, которые были отправлены любым узлом сети 192.168.10.0/24.	`[edit]` `admin@edge# set service nat ipv4 rule 20 source address 192.168.10.0/24`
Применение правила 20 к пакетам, для которых исходящим интерфейсом является `eth3`.	`[edit]` `admin@edge# set service nat ipv4 rule 20 outbound-interface eth3`
Фиксация настройки.	`[edit]` `admin@edge# commit`

Отображение настройки преобразования сетевого адреса отправителя (SNAT).	`[edit]`
	`admin@edge# show service nat`
	`ipv4 {`
	`rule 10 {`
	`outbound-interface eth2`
	`source {`
	`address 192.168.10.0/24`
	`}`
	`type masquerade`
	`}`
	`rule 20 {`
	`outbound-interface eth3`
	`source {`
	`address 192.168.10.0/24`
	`}`
	`type masquerade`
	`}`
	`}`

Добавление маршрута по умолчания в таблицу маршрутизации Gateway_ISP1.	`[edit]` `admin@edge# set protocols static table Gateway_ISP1 route 0.0.0.0/0 next-hop 198.51.100.254`
Добавление маршрута по умолчания в таблицу маршрутизации Gateway_ISP2.	`[edit]` `admin@edge# set protocols static table Gateway_ISP2 route 0.0.0.0/0 next-hop 203.0.113.126`
Фиксация настройки.	`[edit]` `admin@edge# commit`

Отображение настройки маршрутов по умолчанию.	`[edit]`
	`admin@edge# show protocols static`
	`table Gateway_ISP1 {`
	`route 0.0.0.0/0 {`
	`next-hop 198.51.100.254 {`
	`}`
	`}`
	`}`
	`table Gateway_ISP2 {`
	`route 0.0.0.0/0 {`
	`next-hop 203.0.113.126 {`
	`}`
	`}`
	`}`

Создание политики балансировки нагрузки Policy_flow_balancing.	`[edit]` `admin@edge# set policy route Policy_flow_balancing flow-balancing enable`

Действие	Команда
Добавление таблицы маршрутизации Gateway_ISP1 в политику балансировки нагрузки Policy_flow_balancing.	[edit] admin@edge# set policy route Policy_flow_balancing rule 10 table Gateway_ISP1
Добавление таблицы маршрутизации Gateway_ISP2 в политику балансировки нагрузки Policy_flow_balancing.	[edit] admin@edge# set policy route Policy_flow_balancing rule 10 table Gateway_ISP2
Фиксация настройки.	[edit] admin@edge# commit

Отображение настройки политики балансировки нагрузки.	[edit]
	admin@edge# show policy route
	Policy_flow_balancing {
	flow-balancing enable
	rule 10 {
	table Gateway_ISP1 {
	}
	table Gateway_ISP2 {
	}
	}
	}

В примере ниже приведена настройка базовой балансировки нагрузки с указанием типа проверки и целей эхо-запроса.

Пример 333- Настройка базовой балансировки нагрузки

Действие	Команда
Установка значения счетчика сбоев для таблицы маршрутизации Gateway_ISP1 равного 3 (три последовательных сбоя эхо-запроса к удаленным целям).	[edit] admin@edge# set load-balancing table-health Gateway_ISP1 failure-count 3
Установка типа проверки ping для первой цели эхо-запроса для Gateway_ISP1.	[edit] admin@edge# set load-balancing table-health Gateway_ISP1 test 10 type ping
Указание в качестве первой цели эхо-запроса ip-адреса 192.0.2.1 для Gateway_ISP1.	[edit] admin@edge# set load-balancing table-health Gateway_ISP1 test 10 target 192.0.2.1
Установка типа проверки ping для второй цели эхо-запроса для Gateway_ISP1.	[edit] admin@edge# set load-balancing table-health Gateway_ISP1 test 20 type ping
Указание в качестве второй цели эхо-запроса ip-адреса 192.0.2.2 для Gateway_ISP1.	[edit] admin@edge# set load-balancing table-health Gateway_ISP1 test 20 target 192.0.2.2
Установка значения счетчика сбоев для таблицы маршрутизации Gateway_ISP2 равного 5 (пять последовательных сбоев эхо-запроса к удаленным целям).	[edit] admin@edge# set load-balancing table-health Gateway_ISP2 failure-count 5
Установка типа проверки ping для первой цели эхо-запроса для Gateway_ISP2.	[edit] admin@edge# set load-balancing table-health Gateway_ISP2 test 10 type ping
Указание в качестве первой цели эхо-запроса ip-адреса 192.0.2.3 для Gateway_ISP2.	[edit] admin@edge# set load-balancing table-health Gateway_ISP2 test 10 target 192.0.2.3
Установка типа проверки ping для второй цели эхо-запроса для Gateway_ISP2.	[edit] admin@edge# set load-balancing table-health Gateway_ISP2 test 20 type ping

Действие	Команда
Указание в качестве второй цели эхо-запроса ip-адреса 192.0.2.4 для Gateway_ISP2.	[edit] admin@edge# set load-balancing table-health Gateway_ISP2 test 20 target 192.0.2.4
Применение политики балансировки нагрузки для входящего трафика на интерфейсе eth1.	[edit] admin@edge# set interfaces ethernet eth1 policy in route Policy_flow_balancing
Фиксация настройки.	[edit] admin@edge# commit

Отображение настройки балансировки нагрузки.	[edit]
	admin@edge# show load-balancing
	table-health Gateway_ISP1 {
	failure-count 3
	test 10 {
	target 192.0.2.1
	type ping
	}
	test 20 {
	target 192.0.2.2
	type ping
	}
	}
	table-health Gateway_ISP2 {
	failure-count 5
	test 10 {
	target 192.0.2.3
	type ping
	}
	test 20 {
	target 192.0.2.4
	type ping
	}
	}

Использование весов в таблицах маршрутизации

Балансировка нагрузки с учетом весов таблиц маршрутизации выполняется с помощью алгоритма взвешенного случайного распределения. Если веса не назначены, шансы каждой таблицы маршрутизации быть выбранной равны. Если у таблицы маршрутизации больший вес, то в среднем она будет выбрана чаще. Например, если у таблицы маршрутизации Gateway_ISP1 вес 2, а у таблицы маршрутизации Gateway_ISP2 вес 3, таблица маршрутизации Gateway_ISP2 будет выбрана в среднем в 60% случаев.

Данный пример является продолжением вышеприведенных примеров. Для таблиц маршрутизации Gateway_ISP1 и Gateway_ISP2 в правиле 10 политики балансировки нагрузки Policy_flow_balancing указываются веса 20 и 30, соответственно. Для использования весов в таблицах маршрутизации необходимо выполнить следующие действия в режиме настройки:

Пример 334- Настройка использования весов в таблицах маршрутизации

Действие	Команда
Указание веса 20 для таблицы маршрутизации Gateway_ISP1 в политике балансировки нагрузки Policy_flow_balancing.	[edit] admin@edge# set policy route Policy_flow_balancing rule 10 table Gateway_ISP1 weight 20
Указание веса 30 для таблицы маршрутизации Gateway_ISP2 в политике балансировки нагрузки Policy_flow_balancing.	[edit] admin@edge# set policy route Policy_flow_balancing rule 10 table Gateway_ISP2 weight 30
Фиксация настройки.	[edit] admin@edge# commit

Отображение настройки политики балансировки нагрузки.	admin@edge# show policy route
	Policy_flow_balancing {
	flow-balancing enable
	rule 10 {
	table Gateway_ISP1 {
	weight 20
	}
	table Gateway_ISP2 {
	weight 30
	}
	}
	}

Переход на резервную таблицу маршрутизации при неработоспособности остальных таблиц маршрутизации

Данный пример является продолжением примера 334, с учетом добавления резервной таблицы маршрутизации. В предыдущем примере система была настроена на балансировку нагрузки с использованием весов таблиц маршрутизации Gateway_ISP1 и Gateway_ISP2.

В примере 335 в политику балансировки нагрузки Policy_flow_balancing добавляется таблица маршрутизации Gateway_ISP3, которая будет использоваться только в случае неработоспособности маршрутов остальных таблиц маршрутизации, причем трафик, входящий на маршрутизатор Edge через интерфейс eth1, будет передаваться через интерфейс eth4, на котором будет проходить преобразование адресов отправителей (SNAT).

В качестве резервного канала будет использоваться третий поставщик услуг доступа к сети Интернет (203.0.113.254).

Пример настройки балансировки нагрузки с резервным каналом приведен на рисунке ниже.

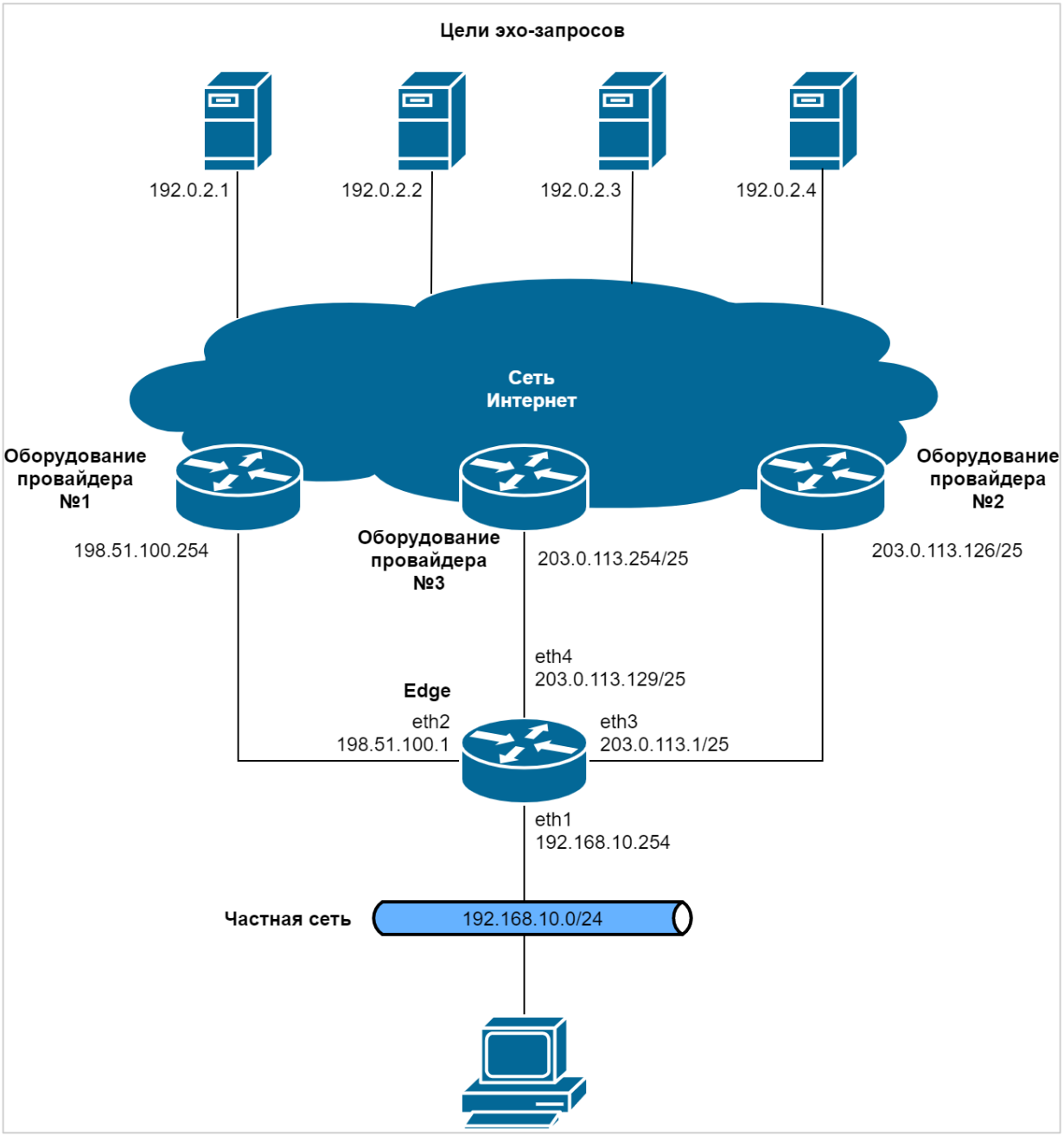


Рисунок 87– Пример настройки балансировки нагрузки с резервным каналом

Для настройки использования резервной таблицы маршрутизации необходимо выполнить следующие действия в режиме настройки:

Пример 335- Настройка использования резервной таблицы при неработоспособности остальных таблиц маршрутизации

Действие	**Команда**
Создание правила 30, преобразующего сетевой адрес отправителя (SNAT).	`[edit]` `admin@edge# set service nat ipv4 rule 30 type masquerade`
Применение правила 30 к пакетам, которые были отправлены любым узлом сети 192.168.10.0/24.	`[edit]` `admin@edge# set service nat ipv4 rule 30 source address 192.168.10.0/24`
Применение правила 30 к пакетам, для которых исходящим интерфейсом является `eth4`.	`[edit]` `admin@edge# set service nat ipv4 rule 30 outbound-interface eth4`
Фиксация настройки.	`[edit]`

Действие	Команда
	admin@edge# commit

Отображение настройки преобразования сетевого адреса отправителя (SNAT) для правила 30.	[edit]
	admin@edge# show service nat ipv4 rule 30
	outbound-interface eth4
	source {
	address 192.168.10.0/24
	}
	type masquerade

Добавление маршрута по умолчания в таблицу маршрутизации Gateway_ISP3.	[edit] admin@edge# set protocols static table Gateway_ISP3 route 0.0.0.0/0 next-hop 203.0.113.254
Добавление таблицы маршрутизации Gateway_ISP3 в политику балансировки нагрузки Policy_flow_balancing в качестве резервной таблицы маршрутизации.	[edit] admin@edge# set policy route Policy_flow_balancing rule 10 table Gateway_ISP3 failover-table
Фиксация настройки.	[edit] admin@edge# commit

Отображение настройки правила 10 политики балансировки нагрузки Policy_flow_balancing.	[edit]
	admin@edge# show policy route Policy_flow_balancing rule 10
	table Gateway_ISP1 {
	weight 20
	}
	table Gateway_ISP2 {
	weight 30
	}
	table Gateway_ISP3 {
	failover-table
	}

38.2 Команды балансировки нагрузки

Команды настройки	
load-balancing table-health <имя_таблицы>	Определение имени таблицы маршрутизации, для которой будет проводиться проверка доступности.
load-balancing table-health <имя_таблицы> failure-count <число>	Установка порогового значения количества сбоев проверок работоспособности таблицы маршрутизации
load-balancing table-health <имя_таблицы> test <номер_теста>	Определение теста работоспособности таблицы маршрутизации.
load-balancing table-health <имя_таблицы> test <номер_теста> resp-time <секунды>	Установка максимального времени ожидания отклика на эхо-запрос, после которого после которого проверка работоспособности считается завершившейся сбоем.Указание ограничения числа транзитных участков для теста типа tll
load-balancing table-health <имя_таблицы> test <номер_теста> target <узел>	Указание целевого узла для проверки работоспособности таблицы маршрутизации.
load-balancing table-health <имя_таблицы> test <номер_теста> ttl-limit <ограничение>	Указание ограничения числа транзитных участков для теста типа tll.
load-balancing table-health <имя_таблицы> test <номер_теста> type <тип>	Указание типа теста для проверки работоспособности таблицы маршрутизации.
load-balancing table-health <имя_таблицы> success-count <число>	Установка количества последовательных успешных проверок работоспособности таблицы маршрутизации.
Эксплуатационные команды	
service load-balance restart	Перезапуск процесса балансировки нагрузки.
service load-balance show	Отображение сведений о таблицах маршрутизации, участвующих в балансировке нагрузки.

service load-balance show connection	Отображение сведений о соединениях, по которым выполняется балансировка нагрузки.

38.2.1 load-balancing table-health <имя_таблицы>

Определение имени таблицы маршрутизации, для которой будет проводиться проверка доступности.

Синтаксис

```
set load-balancing table-health <имя_таблицы>
delete load-balancing table-health <имя_таблицы>
show load-balancing table-health <имя_таблицы>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
load-balancing {
   table-health имя_таблицы {
   }
}
```

Параметры

имя_таблицы

Обязательный. Имя таблицы маршрутизации трафика.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения имени таблицы маршрутизации, для которой будет проводиться проверка доступности.

Форма **set** этой команды используется для указания имени таблицы маршрутизации.

Форма **delete** этой команды используется для удаления имени таблицы маршрутизации.

Форма **show** этой команды используется для отображения имени таблицы маршрутизации.

38.2.2 load-balancing table-health <имя_таблицы> failure-count <число>

Установка порогового значения количества сбоев проверок работоспособности таблицы маршрутизации.

Синтаксис

```
set load-balancing table-health имя_таблицы failure-count <число>
delete load-balancing table-health имя_таблицы failure-count
show load-balancing table-health имя_таблицы failure-count
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
load-balancing {
   table-health имя_таблицы {
      failure-count число
   }
}
```

Параметры

имя_таблицы

Обязательный. Имя таблицы маршрутизации трафика.

число

Пороговое значение закончившихся сбоем проверок работоспособности таблицы маршрутизации. Значение должно лежать в диапазоне от 1 до 10.

Значение по умолчанию

1 сбой. Таким образом после первого же сбоя таблица маршрутизации считается неработоспособной.

Указания по использованию

Эта команда используется для установки порогового значения количества сбоев при проверке работоспособности таблицы маршрутизации.

Форма **set** этой команды используется для установки количества сбоев при проверке работоспособности таблицы маршрутизации.

Форма **delete** этой команды используется для восстановления значения количества сбоев по умолчанию при проверке работоспособности таблицы маршрутизации.

Форма **show** этой команды используется для отображения настройки количества сбоев при проверке работоспособности таблицы маршрутизации.

38.2.3 load-balancing table-health <имя_таблицы> test <номер_теста>

Определение теста работоспособности таблицы маршрутизации.

Синтаксис

```
set load-balancing table-health <имя_таблицы> test <номер_теста>
delete load-balancing table-health <имя_таблицы> test
show load-balancing table-health <имя_таблицы> test
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
load-balancing {
   table-health имя_таблицы {
      test номер_теста {
      }
   }
}
```

Параметры

имя_таблицы

Обязательный. Имя таблицы маршрутизации трафика.

номер_теста

Идентификатор теста.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для определения теста работоспособности таблицы маршрутизации. Для одного теста возможно указать только один целевой узел. Для того чтобы использовать несколько целевых узлов,

необходимо создать соответствующее количество тестов. При наличии нескольких тестов для данной таблицы маршрутизации, они будут выполняться в порядке очереди до получения первого удачного отклика.

Форма **set** этой команды используется для указания узла конфигурации теста.

Форма **delete** этой команды используется для удаления теста.

Форма **show** этой команды используется для отображения настройки теста.

38.2.4 load-balancing table-health <имя_таблицы> test <номер_теста> resp-time <секунды>

Установка максимального времени ожидания отклика на эхо-запрос, после которого проверка работоспособности считается завершившейся сбоем.

Синтаксис

```
set load-balancing table-health <имя_таблицы> test <номер_теста> resp-time <секунды>
delete load-balancing table-health <имя_таблицы> test <номер_теста> resp-time
show load-balancing table-health <имя_таблицы> test <номер_теста> resp-time
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
load-balancing {
    table-health имя_таблицы {
        test номер_теста {
            resp-time секунды
        }
    }
}
```

Параметры

имя_таблицы

Обязательный. Имя таблицы маршрутизации трафика.

номер_теста

Идентификатор теста.

секунды

Временной промежуток (в секундах) ожидания отклика на эхо-запрос, после которого проверка работоспособности таблицы маршрутизации считается завершившейся сбоем. Значение должно лежать в диапазоне от 1 до 30.

Значение по умолчанию

5 секунд. Если сообщение эхо-ответа ICMP в указанное время не получено, считается, что произошел сбой теста с эхо-запросом.

Указания по использованию

Эта команда используется для настройки числа секунд ожидания отклика на эхо-запрос, после которого проверка работоспособности считается завершившейся сбоем.

Форма **set** этой команды используется для установки максимального времени отклика.

Форма **delete** этой команды используется для восстановления времени отклика по умолчанию.

Форма **show** этой команды используется для отображения настройки времени отклика.

38.2.5 load-balancing table-health <имя_таблицы> test <номер_теста> target <узел>

Указание целевого узла для проверки работоспособности таблицы маршрутизации.

Синтаксис

```
set load-balancing table-health <имя_таблицы> test <номер_тест>а target <узел>
delete load-balancing table-health <имя_таблицы> test <номер_теста> target
show load-balancing table-health <имя_таблицы> test <номер_теста> target
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
load-balancing {
   table-health имя_таблицы {
      test номер_теста {
         target узел
      }
   }
}
```

Параметры

имя_таблицы

Обязательный. Имя таблицы маршрутизации трафика.

номер_теста

Идентификатор теста.

узел

IPv4-адрес или имя узла цели проверки работоспособности таблицы маршрутизации.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для настройки получателя сообщений эхо-запросов, отправляемых при проверке работоспособности таблицы маршрутизации. В тесте можно указать только один целевой узел. Для того чтобы использовать несколько целевых узлов, необходимо создать соответствующее количество тестов.

Форма **set** этой команды используется для установки получателя сообщений эхо-запросов, отправляемых при проверке работоспособности таблицы маршрутизации.

Форма **delete** этой команды используется для удаления получателя сообщений эхо-запросов, отправляемых при проверке работоспособности таблицы маршрутизации.

Форма **show** этой команды используется для отображения настройки цели.

38.2.6 load-balancing table-health <имя_таблицы> test <номер_теста> ttl-limit <ограничение>

Указание ограничения числа транзитных участков для теста типа tll.

Синтаксис

```
set load-balancing table-health <имя_таблицы> test <номер_теста> ttl-limit <ограничение>
delete load-balancing table-health <имя_таблицы> test <номер_теста> ttl-limit
show load-balancing table-health <имя_таблицы> test <номер_теста> ttl-limit
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
load-balancing {
   table-health имя_таблицы {
      test номер_теста {
         ttl-limit ограничение
      }
   }
}
```

Параметры

имя_таблицы

Обязательный. Имя таблицы маршрутизации трафика.

номер_теста

Идентификатор теста.

ограничение

Ограничение числа транзитных участков, используемое в случае, если тип теста определен как **ttl**. Значение по умолчанию равно 1.

Значение по умолчанию

Установлено ограничение в один транзитный участок.

Указания по использованию

Эта команда используется для настройки ограничения числа транзитных участков, используемого при проверке работоспособности в тестах типа ttl.

Для успешного прохождения теста, необходимо чтобы ограничение по ttl было короче, чем длина пути до цели, так как для удачного прохождения теста необходимо получение в ответ сообщения ICMP «время истекло».

Форма **set** этой команды используется для указания ограничения числа транзитных участков, используемого в тестах при проверке работоспособности.

Форма **delete** этой команды используется для удаления ограничения числа транзитных участков.

Форма **show** этой команды используется для отображения настройки ttl-limit.

38.2.7 load-balancing table-health <имя_таблицы> test <номер_теста> type <тип>

Указание типа теста для проверки работоспособности таблицы маршрутизации.

Синтаксис

```
set load-balancing table-health <имя_таблицы> test <номер_теста> type <тип>
delete load-balancing table-health <имя_таблицы> test <номер_теста> type
show load-balancing table-health <имя_таблицы> test <номер_теста> type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
load-balancing {
   table-health имя_таблицы {
      test номер_теста {
         type тип
```

```
        }
    }
}
```

Параметры

имя_таблицы

Обязательный. Имя таблицы маршрутизации трафика.

номер_теста

Идентификатор теста.

тип

Тип выполняемого теста. Поддерживаются следующие значения:

ping: Выполнение теста с эхо-запросом.

ttl: Выполнение теста по UDP.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания выполняемого типа теста проверки работоспособности.

В тестах типа ping, на удаленную точку назначения отправляется сообщение эхо-запроса ICMP («пинга»). В случае успешного ответа от точки назначения, таблица маршрутизации признается прошедшей тест на проверку работоспособности. В случае сбоя проверки работоспособности, таблица маршрутизации удаляется из пула активных таблиц маршрутизации.

В тестах типа ttl, на удаленную точку назначения отправляется пакет UDP с ограничением по времени жизни. Для успешного прохождения теста, необходимо чтобы ограничение по ttl было короче, чем длина пути до цели, так как для удачного прохождения теста необходимо получение в ответ сообщения ICMP «время истекло».

Форма **set** этой команды используется для указания выполняемого типа теста проверки работоспособности.

Форма **delete** используется для удаления настройки типа теста проверки работоспособности.

Форма **show** этой команды используется для отображения настройки типа теста проверки работоспособности.

38.2.8 load-balancing table-health <имя_таблицы> success-count <число>

Установка количества последовательных успешных проверок работоспособности таблицы маршрутизации.

Синтаксис

```
set load-balancing table-health <имя_таблицы> success-count <число>
delete load-balancing table-health <имя_таблицы> success-count
show load-balancing table-health <имя_таблицы> success-count
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
load-balancing {
    table-health имя_таблицы {
        success-count число
    }
}
```

Параметры

имя_таблицы

Обязательный. Имя таблицы маршрутизации трафика.

число

Число последовательных успешных откликов в тестах, необходимое для возврата указанной таблицы маршрутизации в пул активных таблиц маршрутизации. Значение должно лежать в диапазоне от 1 до 10. Значение по умолчанию равно 1.

Значение по умолчанию

Если таблица маршрутизации успешно выполняет один тестовый цикл, она возвращается в пул активных таблиц маршрутизации, участвующих в балансировке нагрузки.

Указания по использованию

Эта команда используется для установки числа последовательных успешных проверок работоспособности таблицы маршрутизации.

Форма **set** этой команды используется для указания числа последовательных успешных откликов.

Форма **delete** этой команды используется для восстановления числа последовательных успешных откликов по умолчанию.

Форма **show** этой команды используется для отображения настройки числа последовательных успешных откликов.

38.2.9 service load-balance restart

Перезапуск процесса балансировки нагрузки.

Синтаксис

```
service load-balance restart
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для перезапуска процесса балансировки нагрузки.

38.2.10 service load-balance show

Отображение сведений о таблицах маршрутизации, участвующих в балансировке нагрузки.

Синтаксис

```
service load-balance show
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для вывода сведений о таблицах маршрутизации, участвующих в балансировке нагрузки. Команда отображает сведения по каждой таблице маршрутизации и выдает отчет о текущем состоянии.

Кроме того, команда выводит типы и цели тестов (в порядке настроенных номеров тестов).

Примеры

В примере приведены сведения о таблицах маршрутизации, участвующих в балансировке нагрузки.

Пример 336- Отображение сведений о таблицах маршрутизации, участвующих в балансировке нагрузки

```
admin@edge:~$ service load-balance show
Table: TABLE1
       Status: active
       Last Status Change: unknown
       Last Table Success: Thu Jul 23 13:23:57 2020
       Last Table Failure: Thu Jul 23 13:14:37 2020
       Failures count: 0 of 5
       Successes count: 1 of 1
       Rule: ping 192.168.100.254
       Status: success
```

38.2.11 service load-balance show connection

Отображение сведений о соединениях, по которым выполняется балансировка нагрузки.

Синтаксис

```
service load-balance show connection
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для вывода сведений о соединениях, касающихся трафика, по которому балансируется нагрузка.

Примеры

В примере приведены сведения о соединениях, участвующих в балансировке нагрузки.

Пример 337 - Отображение сведений о соединениях, касающихся балансировки нагрузки

```
admin@edge:~$ service load-balance show connection
Type State      Src                Dst              Packets Bytes

tcp ESTABLISHED 192.168.10.1:54066 203.0.113.1:5001 36462 317232760

tcp ESTABLISHED 192.168.10.1:54068 203.0.113.1:5001 35464 295146288

icmp            192.168.10.1       203.0.113.1      2     168
```

Межсетевой экран Numa Edge

Руководство администратора

Построение виртуальных частных сетей (VPN) на основе протокола OpenVPN

Листов 88

Санкт-Петербург
2022

Содержание

ИДЕНТИФИКАЦИЯ ДОКУМЕНТА

Название документа	Руководство администратора. Построение виртуальных частных сетей (VPN) на основе протокола OpenVPN
Версия документа	1.7
Обозначение документа	643.АМБН.00004-01 32 02
Идентификация ОО	Межсетевой экран Numa Edge
Идентификация разработчика	ООО «НумаТех»
Ключевые слова	Межсетевой экран, МЭ, OpenVPN

АННОТАЦИЯ ДОКУМЕНТА

Документ предназначен для ознакомления пользователя с технической информацией о настройке виртуальных частных сетей на основе набора протокола OpenVPN в межсетевом экране Numa Edge (далее – Изделие или Numa Edge) и содержит сведения о примерах и командах настройки.

1 МЕХАНИЗМЫ БЕЗОПАСНОСТИ OPENVPN

В данном разделе представлен краткий обзор механизмов безопасности и режимов эксплуатации OpenVPN.

К требованиям безопасности при использовании виртуальных частных сетей относятся обеспечение проверки подлинности, конфиденциальности и целостности. В OpenVPN могут быть использованы два различных механизма безопасности: с использованием статических ключей и протокола TLS (transport layer security).

ПРИМЕЧАНИЕ. SSL является предшественником TLS, и в настоящее время в большинстве случаев при упоминании SSL в действительности подразумевается TLS. По этой причине в данном документе эти термины являются взаимозаменяемыми.

2 ИСПОЛЬЗОВАНИЕ СКЗИ «МАГПРО КРИПТОПАКЕТ» ВЕРСИЯ 4.0

В Numa Edge имеется возможность использования СКЗИ «МагПро КриптоПакет» версия 4.0 (СЕИУ.00009-05) в исполнении «OpenVPN-ГОСТ» (исполнение 7).

«МагПро КриптоПакет» 4.0 в исполнении «OpenVPN-ГОСТ» реализует следующие функции:

- создание и проверку электронной подписи в соответствии с ГОСТ Р 34.10 для файлов и данных, содержащихся в областях оперативной памяти;
- зашифрование и расшифрование в соответствии с ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015 и ГОСТ 28147-89 (только для взаимодействия с ПО, не поддерживающим ГОСТ Р 34.12-2015) файлов и данных, содержащихся в областях оперативной памяти;
- имитозащиту в соответствии с ГОСТ Р 34.13-2015, HMAC на основе ГОСТ Р 34.11-2012, а также ГОСТ 28147-89 (только для взаимодействия с ПО, не поддерживающим ГОСТ Р 34.13-2015) файлов и данных, содержащихся в областях оперативной памяти;
- вычисление ключа парной связи по алгоритму VKO с использованием как эфемерных, так и долговременных пар закрытых и открытых ключей, созданных в соответствии с ГОСТ Р 34.10;
- вычисление значения хэш-функции в соответствии с ГОСТ Р 34.11 для файлов и данных, содержащихся в областях оперативной памяти;
- выработку случайного числа заданной длины;
- вычисление открытых и закрытых ключей проверки подписи в соответствии с ГОСТ Р 34.10;
- формирование производного сеансового ключа;
- импорт криптографических ключей в СКЗИ и их экспорт из СКЗИ;
- реализацию протокола TLS с использованием российских криптонаборов, определенных реализациями ТК26.

При использовании Numa Edge с СКЗИ «МагПро КриптоПакет» должны соблюдаться требования следующих документов:

- СЕИУ.00009-05 30. Формуляр;
- СЕИУ.00009–05 94. Правила пользования.

Конфигурирование виртуальной частной сети «OpenVPN-ГОСТ» (СКЗИ «МагПро КриптоПакет») осуществляется через стандартную систему конфигурирования Numa Edge и в целом не отличается от использования OpenVPN с общемировыми алгоритмами. Применение СКЗИ «МагПро КриптоПакет» 4.0 осуществляется при выборе специальных алгоритмов шифрования в блоке конфигурирования интерфейса OpenVPN **interfaces openvpn <vtunx> encryption <алгоритм>**. Алгоритмы (<algo>), при которых для построения VPN будет использоваться непосредственно СКЗИ «МагПро КриптоПакет», отмечены суффиксом «-cc» (например, gost89-cc и magma-mgm-cc. За более подробным описанием обратитесь к документации соответствующего узла конфигурации).

При первом запуске сервиса OpenVPN с СКЗИ «МагПро КриптоПакет» 4.0 будет запущено создание файла инициализации программного датчика случайных чисел с использованием утилиты mkseed (СЕИУ.00009-05 34 10. Программа генерации файла инициализации программного ДСЧ mkseed. Руководство по использованию).

ВНИМАНИЕ. В каждом Изделии на производстве устанавливается уникальная лицензия СКЗИ «МагПро КриптоПакет», привязанная к аппаратной платформе. При переустановке

Изделия с дистрибутива на компакт-диске или сброса Изделия к заводским настройкам из меню загрузки лицензия на СКЗИ «МагПро КриптоПакет» будет утеряна. Обратитесь в службу технической поддержки производителя для ее восстановления.

ВНИМАНИЕ. При использовании СКЗИ «МагПро КриптоПакет» не рекомендуется изменять MAC-адреса физических интерфейсов платформы Numa Edge. Одновременное изменение MAC-адресов всех физических интерфейсов платформы приведет к невозможности проверки лицензии на СКЗИ «МагПро КриптоПакет».

3 ТРЕБОВАНИЯ К ПРОЦЕДУРАМ АДМИНИСТРИРОВАНИЯ

При использовании Numa Edge с СКЗИ «МагПро КриптоПакет» управление Изделия должно осуществляться при помощи специализированного автоматизированного рабочего места администратора (далее – АРМ администратора).

Конфигурирование Numa Edge с АРМ администратора может осуществляться следующими способами:

- локально, путем подключения по последовательному интерфейсу RS-232;
- удаленно по протоколу SSH;
- удаленно через веб-интерфейс по протоколам HTTP/HTTPS.

Удаленное управление должно производиться по безопасным каналам, а именно:

- из контролируемой зоны по незащищенному каналу только при невозможности подключения к этому каналу нарушителя;
- из-за пределов контролируемой зоны или при возможности подключения к каналу нарушителя – только по защищенным с использованием сертифицированного ФСБ СКЗИ соединениям.

При использовании незащищенных управляющих соединений АРМ администратора должно размещаться в отдельном сегменте сети, защищенном от доступа посторонних лиц, и подключаться к управляемому Numa Edge через выделенный физический сетевой интерфейс.

Запрещается установление незащищенных управляющих соединений по беспроводным каналам связи.

При первом сеансе конфигурирования Numa Edge администратору необходимо:

- создать необходимые учетные записи администраторов и операторов Numa Edge;
- установить пароли учетным записям администраторов Numa Edge, от имени которых может осуществляться конфигурирование (управление), устанавливаемые пароли должны соответствовать требованиям СЕИУ.00009–05 94 «Средство криптографической защиты информации «МагПро КриптоПакет» 4.0. Правила пользования»;
- предустановленная учетная запись администратора должна быть удалена, деактивирована или для нее должен быть установлен пароль, соответствующий требованиям, указанным выше, либо отключена парольная аутентификация;
- при получении конфигурационного файла из сторонних источников он должен передаваться по надежному каналу, исключающему его искажение. В противном случае администратор должен иметь возможность убедиться в целостности получаемой конфигурации любым иным способом.

Требования к АРМ администратора:

- на АРМ администратора следует устанавливать только лицензионное программное обеспечение фирм-изготовителей, необходимое для целей управления;
- на АРМ администратора должна быть установлена коммуникационная программа (например, HyperTerminal или putty для ОС Windows, minicom для ОС Linux), позволяющая работать с соединениями по последовательному интерфейсу RS-232 (в том числе эмулируемому) и/или сетевому соединению по протоколу ssh;
- АРМ администратора должно быть защищено от НСД сертифицированными ФСБ России средствами, сертифицированными ФСТЭК России средствами или организационно-техническими мерами, исключающими доступ к ним посторонних лиц;

- АРМ администратора должно быть защищено от воздействия вредоносного кода сертифицированными ФСБ России средствами, сертифицированными ФСТЭК России средствами или организационно-техническими мерами, обеспечивающими невозможность воздействия вредоносного кода;
- в отношении АРМ администратора должны выполняться требования по защите от НСД, в том числе администратором безопасности должен осуществляться периодический контроль целостности установленного ПО (включая коммуникационную программу);
- в отношении АРМ администратора необходимо предусмотреть меры, исключающие возможность несанкционированного и необнаруживаемого изменения аппаратной части технических средств;
- на АРМ администратора запрещается устанавливать средства разработки ПО и отладчики. Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано администратором безопасности.

Программное обеспечение, устанавливаемое на АРМ администратора, за исключением являющегося частью ОС или средствами защиты информации, такими как СКЗИ, антивирусное ПО, СЗИ от НСД и др., не должно содержать возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;
- модифицировать собственный код и код других подпрограмм;
- модифицировать память, выделенную для других подпрограмм;
- передавать управление в область собственных данных и данных других подпрограмм;
- несанкционированно модифицировать файлы, содержащие исполняемые коды, при их хранении на жестком диске;
- повышать предоставленные привилегии;
- несанкционированно модифицировать настройки ОС;
- использовать недокументированные фирмой-разработчиком функции ОС.

Хранение настроек (конфигураций) Numa Edge на АРМ администратора допускается только при условии обеспечения контроля их целостности и разграничении права доступа к ним, ограничивающим доступ для всех пользователей, за исключением уполномоченных администраторов.

4 СТАТИЧЕСКИЕ КЛЮЧИ

ПРИМЕЧАНИЕ. Механизм шифрования со статическим ключем несовместим с ГОСТ алгоритмами, соответственно, при их использовании возможно осуществление шифрования только используя механизм TLS.

При использовании статических ключей OpenVPN функционирует следующим образом:

1) администратор, используя команду эксплуатационного режима *vpn openvpn-key generate <имя_ключа>*, генерирует файл, содержащий определенное число случайных байтов данных. Эти данные представляют собой секретный ключ, часть данных которого будут использоваться для шифрования и расшифровки передаваемых данных, а часть данных для проверки целостности этих данных. Поскольку эти ключи получаются из файла и не изменяются в течение всего срока действия соединения (в отличие от режима TLS), данные ключи называются статическими;

2) администратор передает секретный файл каждому из двух оконечных устройств, используя заранее установленный безопасный канал. Например, файл может быть создан на одном из двух оконечных устройств и затем передан на другое устройство при помощи защищенного протокола передачи файлов, например, такого как SCP. Поскольку наличие этого общего ключа на каждом из устройств является обязательным условием для установления защищенного соединения, он также называется предварительно-распределённым ключом;

3) когда потребуется установить туннель VPN между оконечными устройствами, OpenVPN на одном оконечном устройстве осуществляет проверку подлинности другого оконечного устройства. Проверка подлинности осуществляется на основе предположения, что статический ключ известен только второму оконечному устройству; то есть проверка подлинности осуществляется исходя из предположения, что если некоторому устройству известен предварительно-распределенный ключ, то это устройство является правомерным оконечным устройством;

4) после осуществления проверки подлинности оконечных узлов, OpenVPN формирует на каждой из сторон набор ключей из предварительно-распределенного ключа. Данные ключи используются в следующих целях:

- некоторые из них используются для шифрования данных, передаваемых через туннель, что позволяет обеспечить конфиденциальность;
- другие используются в кодах аутентификации сообщений (MAC, message authentication code), которые применяют ключевой хэш-алгоритм к данным, передаваемым через туннель, что позволяет обеспечить целостность.

5 TLS

TLS — криптографический протокол, обеспечивающий защищённую передачу данных между узлами в сети Интернет, не требующий наличия предварительно-распределенного ключа. TLS предоставляет возможности аутентификации и безопасной передачи данных через Интернет с использованием криптографических средств. Для взаимной аутентификации каждая из сторон должна поддерживать инфраструктуру открытых ключей (PKI).

OpenVPN использует TLS с сертификатами стандарта X.509 и требует наличия инфраструктуры открытых ключей (PKI) для генерации сертификатов. При использовании TLS OpenVPN работает следующим образом:

1) используя инфраструктуру открытых ключей, администратор создает сертификаты и связывает их с оконечными узлами. Все сертификаты подписываются удостоверяющим центром (CA). Сертификат оконечного устройства содержит необходимые сведения об узле, в том числе имя оконечного устройства, которое указано в поле Common Name сертификата;
2) администратор передает каждый сертификат и связанные с ним файлы на соответствующее оконечное устройство, используя заранее установленное безопасное соединение, например, SCP;
3) при установке туннеля VPN между оконечными устройствами, одно из них имеет пассивную роль, а другое – активную, и соответственно устанавливает TLS-соединение с пассивным устройством;
4) после установления соединения TLS обе стороны осуществляют проверку подлинности друг друга, используя свою пару открытого и секретного ключа, а также открытый ключ удостоверяющего центра, который известен обоим оконечным устройствам;
5) после осуществления проверки подлинности устанавливается разделяемый секретный ключ при помощи асимметричных криптографических алгоритмов. Каждое оконечное устройство после этого получает набор сеансовых ключей. Как и в случае с механизмом безопасности, использующим статические ключи, сеансовые ключи затем используются для шифрования данных и аутентификации сообщений (MAC), передаваемых через туннель, для обеспечения целостности и конфиденциальности. Однако в отличие от механизма безопасности, использующего статические ключи, сеансовые ключи используются только для одного сеанса и, соответственно, называются сеансовыми ключами. Для каждого последующего сеанса вырабатывается новый набор сеансовых ключей.

Создание и распределение сертификатов с использованием PKI включает в себя множество вопросов, связанных с обеспечением безопасности, рассмотрение которых выходит за рамки данного документа.

6 ИСПОЛЬЗОВАНИЕ РАСШИРЕНИЙ СЕРТИФИКАТОВ X.509

Для того чтобы избежать возможных атак типа «человек посередине», при подключении клиентского узла к другому клиентскому узлу, выдающему себя за сервер, рекомендуется использовать в сертификатах узлов VPN расширение ExtendedKeyUsage (значения clientAuth и serverAuth). Для получения подробных сведений об использовании расширений сертификатов см. RFC3280.

ПРИМЕЧАНИЕ. Расширение ExtendedKeyUsage позволяет указать одну или более целей использования открытого ключа в дополнение к целям, заданным в расширении KeyUsage. При наличии данных расширений сертификат может быть использован только с указанными целями.

Таким образом, следует учитывать, что если в используемом сертификате узла используется расширение ExtendedKeyUsage, и в этом расширении не указано значение clientAuth (или serverAuth), то удаленный сертификат будет признан недопустимым для использования по назначению и его проверка завершится с ошибкой.

7 МЕЖФИЛИАЛЬНЫЙ РЕЖИМ

На рисунке 1 представлен простой пример межфилиального подключения на базе OpenVPN. Данный пример может быть использован, например, для установки соединения между удаленным офисом и центром обработки данных.

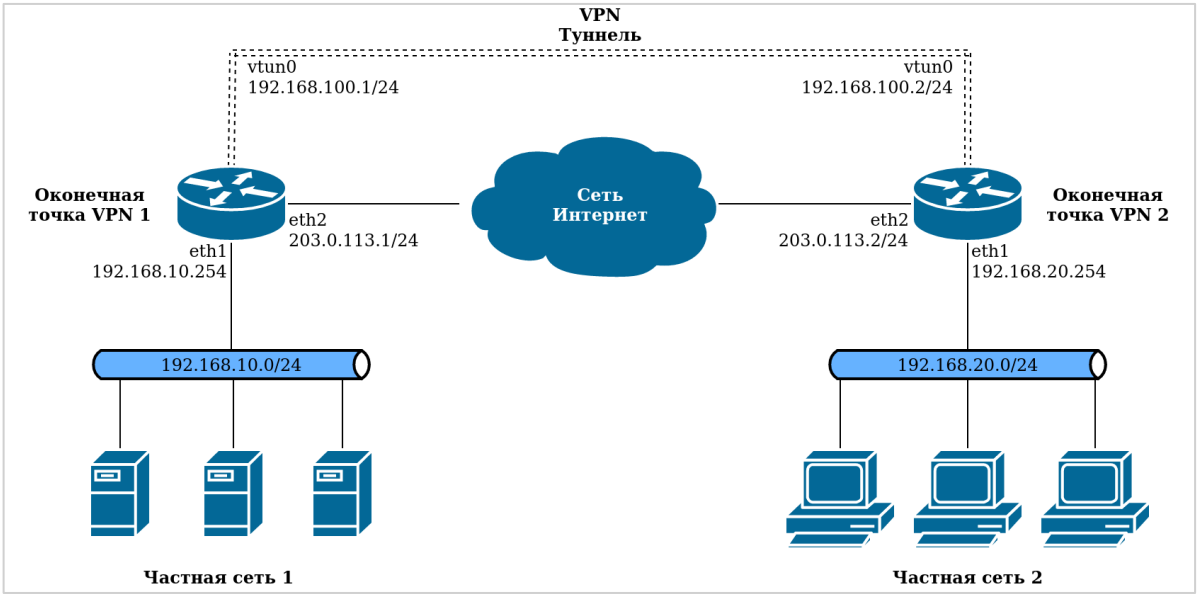


Рисунок 1 – VPN в межфилиальном режиме на базе OpenVPN

В каждой оконечной точке туннеля VPN процесс OpenVPN создает маршрутизируемый «туннельный интерфейс» и устанавливает защищенный туннель с другим оконечным устройством. Соответственно, оба интерфейса принадлежат одной и той же подсети, хотя пакеты, передаваемые между этими двумя интерфейсами, в действительности обрабатываются и отправляются через защищенный туннель процессом OpenVPN.

Следует отметить, что на каждом оконечном устройстве установлены два IP-адреса:

- туннельный IP-адрес: виртуальный адрес (VIP) на каждой оконечной точке туннеля. IP-адреса на каждой из оконечных точек туннеля должны лежать в одной подсети. В примере, представленном на рисунке 1, IP-адресами туннеля являются адреса 192.168.100.1 и 192.168.100.2;
- физический IP-адрес: IP-адрес, назначаемый физическому интерфейсу, поверх которого устанавливается туннель VPN. В данном примере физическими IP-адресами являются адреса 203.0.113.1 и 203.0.113.2.

В большинстве случаев туннель VPN используется для передачи трафика между частными подсетями через глобальную вычислительную сеть (WAN). В текущем примере частные сети 192.168.10.0/24 и 192.168.20.0/24 расположены за оконечными узлами туннеля VPN. При этом на каждом оконечном устройстве следует добавить статический маршрут, направляющий трафик от и к удаленной частной подсети через туннельный интерфейс.

При использовании межфилиального режима одно и то же устройство может установить несколько туннелей к различным точкам. Даже в том случае, если несколько туннелей используют один и тот же физический интерфейс, каждый туннель представлен отдельным IP-адресом туннельного интерфейса и функционирует независимо.

8 ПРИМЕРЫ БАЗОВОЙ НАСТРОЙКИ

В данном разделе приведены несколько основных вариантов использования OpenVPN, а также описания их настройки. В этом разделе рассматриваются следующие вопросы:

- Межфилиальный режим с использованием статических ключей;
- Межфилиальный режим с использованием TLS;
- Клиент-серверный режим;
- Настройка межсетевого экрана.

8.1 Межфилиальный режим с использованием статических ключей

На рисунке 2 приведен вариант подключения VPN в межфилиальном режиме между узлами Edge1 и Edge2 с использованием статических ключей. В данном примере:

- физические IP-адреса для узлов Edge1 и Edge2 – 203.0.113.1 и 203.0.113.2 соответственно;
- туннельные IP-адреса для узлов Edge1 и Edge2 – 192.168.100.1 и 192.168.100.2 соответственно;
- подсети, между которыми организуется взаимодействие:
  - подсеть, которая расположена за узлом Edge1 – 192.168.10.0/24;
  - подсеть, которая расположена за узлом Edge2 – 192.168.20.0/24;
- статический ключ заранее создан при помощи команды *vpn openvpn-key generate <имя_ключа>*, где <имя_ключа> – имя секретного ключа, используемое в дальнейшем.

Для настройки туннеля OpenVPN следует создать туннельный интерфейс. Имя интерфейса имеет следующий формат **vtun** *номер*; например, vtun0, vtun1 и так далее. В дополнение необходимо добавить статический маршрут для интерфейса, который будет направлять трафик, предназначенный для удаленной подсети через туннельный интерфейс **vtun0**.

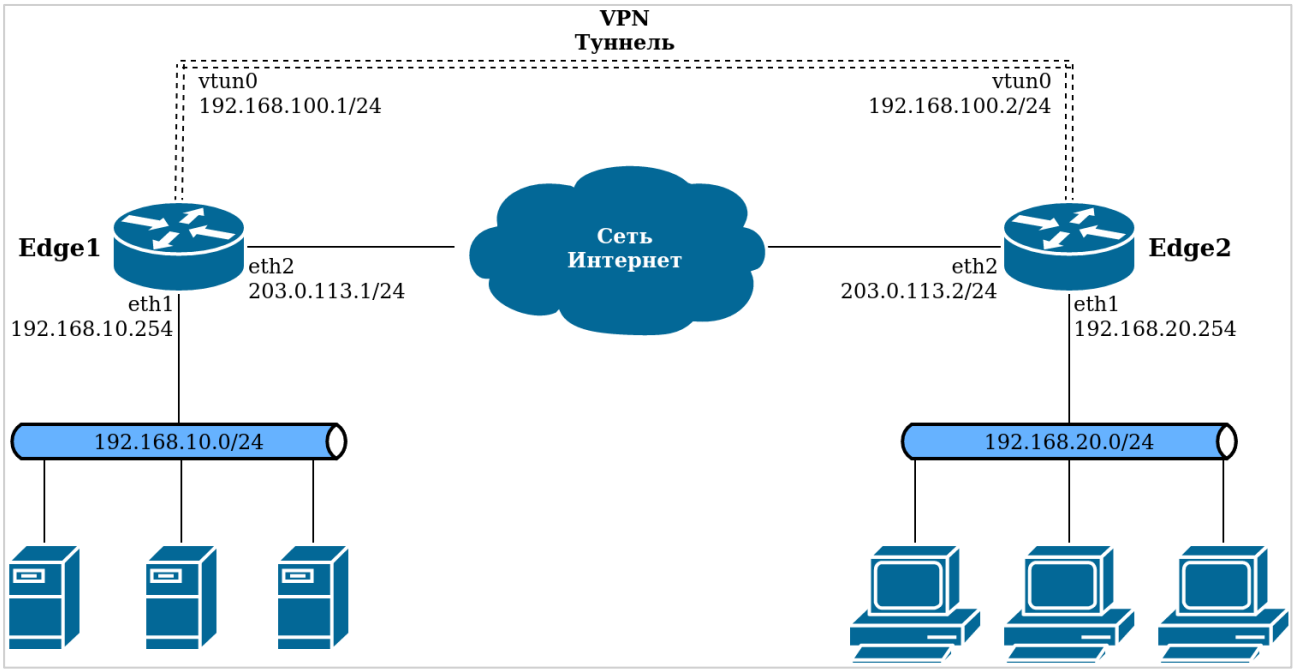


Рисунок 2 – Пример подключения в межфилиальном режиме между узлами Edge1 и Edge2 с использованием статических ключей

В этом разделе представлены следующие примеры:

- пример 2.1 – Межфилиальный режим с использованием статических ключей: оконечное устройство Edge1;

- пример 2.2 – Межфилиальный режим с использованием статических ключей: статический маршрут Edge1;
- пример 2.4 – Межфилиальный режим с использованием статических ключей: оконечное устройство Edge2;
- пример 2.5 – Межфилиальный режим с использованием статических ключей: статический маршрут Edge2.

Для настройки оконечного устройства Edge1 следует выполнить указанные шаги в режиме настройки.

Пример 2.1 – Межфилиальный режим с использованием статических ключей: оконечное устройство Edge1

Действие	**Команда**
Создание узла конфигурации vtun0	[edit] admin@Edge1# set interfaces openvpn vtun0
Назначение туннельного IP-адреса локальному оконечному устройству	[edit] admin@Edge1# set interfaces openvpn vtun0 local-address 192.168.100.1
Установка межфилиального режима OpenVPN	[edit] admin@Edge1# set interfaces openvpn vtun0 mode site-to-site
Назначение туннельного IP-адреса удаленного оконечного устройства	[edit] admin@Edge1# set interfaces openvpn vtun0 remote-address 192.168.100.2
Указание физического IP-адреса удаленного устройства	[edit] admin@Edge1# set interfaces openvpn vtun0 remote-host 203.0.113.2
Указание расположения файла, содержащего статический ключ	[edit] admin@Edge1# set interfaces openvpn vtun0 shared-secret-key secret
Указание используемого алгоритма шифрования	[edit] admin@Edge1# set interfaces openvpn vtun0 encryption aes256
Фиксация изменений	[edit] admin@Edge1# commit
Вывод настройки OpenVPN	[edit] admin@Edge1# show interfaces openvpn vtun0 encryption aes256 local-address 192.168.100.1 mode site-to-site remote-address 192.168.100.2

Действие	Команда
	remote-host 203.0.113.2 shared-secret-key secret

Для настройки статического маршрута к удаленной подсети через туннель OpenVPN, необходимо выполнить следующие шаги в режиме настройки.

Пример 2.2 – Межфилиальный режим с использованием статических ключей: статический маршрут на узле Edge1

Действие	Команда
Создание статического маршрута для получения доступа к удаленной подсети через туннель OpenVPN	[edit] admin@Edge1# set protocols static interface-route 192.168.20.0/24 next-hop-interface vtun0
Фиксация изменений	[edit] admin@Edge1# commit

Вывод статических маршрутов	[edit]
	admin@Edge1# show protocols static
	interface-route 192.168.20.0/24 {
	next-hop-interface vtun0
	}

Настройка оконечного устройства VPN Edge2 аналогична настройке Edge1 за исключением того, что локальный и удаленный туннельные IP-адреса меняются местами. Предварительно на устройство Edge2 необходимо передать файл, содержащий статический ключ, при этом следует помнить, что статический ключ следует сохранять в секрете и для его передачи должны использоваться только защищенные каналы. Например, файл статического ключа можно передать на другое оконечное устройство с использованием флэш-накопителя или протокола SCP. Для передачи файла статического ключа по протоколу SCP следует выполнить на устройстве Edge1 следующую команду:

```
vpn openvpn-key export <имя_ключа> to scp://<пользователь>@<ip-адрес>/<путь_к_файлу>
```

где

- имя_ключа – имя статического ключа;
- пользователь – имя пользователя на устройстве Edge2;
- ip-адрес – IP-адрес устройства Edge2;
- путь_к_файлу – путь к файлу на устройстве Edge2, куда будет скопирован ключ.

После доставки файла статического ключа на устройство Edge2 его необходимо импортировать. Для этого следует выполнить команду:

```
vpn openvpn-key import <имя_ключа> from <путь_к_файлу>
```

где

- имя_ключа – имя статического ключа, под которым он будет сохранен в системе;
- путь_к_файлу – путь к файлу на локальном устройстве.

После чего скопированный ранее файл ключа на носителе устройства Edge2 рекомендуется удалить.

В примере 2.3 приведен экспорт файла статического ключа на устройство Edge2 по протоколу SCP и его импорт под именем openvpn_key.

Пример 2.3 – Экспорт и импорт файла статического ключа по протоколу SCP

```
admin@edge1:~$ vpn openvpn-key export <имя_ключа> to
scp://admin@203.0.113.2/home/admin/secret
admin@edge2:~$ vpn openvpn-key import openvpn_key from secret
```

Для настройки оконечного устройства Edge2 необходимо выполнить следующие шаги в режиме настройки.

Пример 2.4 – Межфилиальный режим с использованием статических ключей: оконечное устройство Edge2

Действие	Команда
Создание узла конфигурации vtun0	[edit] admin@Edge2# set interfaces openvpn vtun0
Назначение туннельного IP-адреса локальному оконечному устройств	[edit] admin@Edge2# set interfaces openvpn vtun0 local-address 192.168.100.2
Установка межфилиального режима OpenVPN	[edit] admin@Edge2# set interfaces openvpn vtun0 mode site-to-site
Назначение туннельного IP-адреса удаленного оконечного устройства	[edit] admin@Edge2# set interfaces openvpn vtun0 remote-address 192.168.100.1
Указание физического IP-адреса удаленного устройства	[edit] admin@Edge2# set interfaces openvpn vtun0 remote-host 203.0.113.1
Указание расположения файла, содержащего статический ключ	[edit] admin@Edge2# set interfaces openvpn vtun0 shared-secret-key openvpn_key
Указание используемого алгоритма шифрования	[edit] admin@Edge2# set interfaces openvpn vtun0 encryption aes256
Фиксация изменений	[edit] admin@Edge2# commit
Вывод настройки OpenVPN	[edit] admin@Edge2# show interfaces

Действие	Команда
	openvpn vtun0 encryption aes256 local-address 192.168.100.2 mode site-to-site remote-address 192.168.100.1 remote-host 203.0.113.1 shared-secret-key openvpn_key

Разделяемый секретный файл должен быть один и тот же на обоих оконечных узлах (при этом имя ключа может быть различным, как продемонстрировано в примере выше). Следует отметить, что параметр **remote-host** требуется только на одном из оконечных устройств; таким образом, межфилиальный туннель VPN может быть установлен при условии наличия хотя бы у одного из оконечных устройств достаточной информации для установки соединения с другим.

Для настройки статического маршрута к удаленной подсети через туннель OpenVPN, необходимо выполнить следующие шаги в режиме настройки.

Пример 2.5 – Межфилиальный режим OpenVPN с использованием статических ключей: статический маршрут на узле Edge2

Действие	Команда
Создание статического маршрута для получения доступа к удаленной подсети через туннель OpenVPN	[edit] admin@Edge2# set protocols static interface-route 192.168.10.0/24 next-hop-interface vtun0
Фиксация изменений	[edit] admin@Edge2# commit

Вывод настройки статических маршрутов	[edit]
	admin@Edge2# show protocols static interface-route 192.168.10.0/24 {
	next-hop-interface vtun0
	}

8.2 Межфилиальный режим с использованием TLS

При использовании TLS в межфилиальном режиме настройка аналогична приведенной в предыдущем разделе за исключением того, что необходимо настроить параметры, относящиеся к TLS, вместо параметра **shared-secret-key**. Как было указано выше, одно оконечное устройство выполняет пассивную роль, а другое – активную роль.

Следующая настройка аналогична настройке, приведенной в предыдущем разделе. Для использования TLS необходимо предварительно сгенерировать сертификаты x509 для каждого из устройств. Для их генерации может использоваться внутренний удостоверяющий центр Numa Edge. Предполагается, что Edge1 и Edge2 исполняют пассивную и активную роль соответственно, генерация x509 сертификатов осуществляется на устройстве Edge1.

Для генерации сертификатов x509 необходимо выполнить следующие действия:

Пример 2.6 – Edge1 – Генерация сертификатов для межфилиального режима VPN с использованием TLS

Действие	Команда
Создание удостоверяющего центра	[edit] admin@Edge1# set pki ca MainCA
Указание общего имени (common name) удостоверяющего центра	[edit] admin@Edge1# set pki ca MainCA cn "Main Certification Authority"
Указание города в качестве одного из атрибутов идентификатора УЦ	[edit] admin@Edge1# set pki ca MainCA city SPb
Указание страны в качестве одного из атрибутов идентификатора УЦ	[edit] admin@Edge1# set pki ca MainCA country RU
Указание периода действия сертификата удостоверяющего центра	[edit] admin@Edge1# set pki ca MainCA expiration 1095
Фиксация настройки	[edit] admin@Edge1# commit
Вывод настройки	[edit] admin@Edge1# show -all pki ca MainCA city SPb cn "Main Certification Authority" country RU expires-on "Thu Nov 7 12:35:42 2021" key-size 256 key-type gost2012
Создание сертификата для узла Edge1	[edit] admin@Edge1# set pki ca MainCA certificate Edge1-cert
Указание общего имени (common name), которое будет указано в сертификате узла Edge1	[edit] admin@Edge1# set pki ca MainCA certificate Edge1-cert cn "Edge1-cert"
Указание срока действия сертификата. Срок действия выпускаемого сертификата не должен превышать срок действия сертификата УЦ	[edit] admin@Edge1# set pki ca MainCA certificate Edge1-cert expiration 365

Действие	Команда
Создание сертификата для узла Edge2	[edit] admin@Edge1# set pki ca MainCA certificate Edge2-cert
Указание общего имени (common name), которое будет указано в сертификате узла Edge2	[edit] admin@Edge1# set pki ca MainCA certificate Edge2-cert cn "Edge2-cert"
Указание срока действия сертификата. Срок действия выпускаемого сертификата не должен превышать срок действия сертификата УЦ	[edit] admin@Edge1# set pki ca MainCA certificate Edge2-cert expiration 365
Фиксация настройки	[edit] admin@Edge1# commit

Вывод настройки созданных сертификатов	[edit]
	admin@Edge1# show pki ca MainCA certificate
	Edge1-cert {
	cn "Edge1 VPN Peer certificate"
	expires-on "Thu Nov 14 11:20:48 2019"
	key-size 256
	key-type gost2012
	}
	Edge2-cert {
	cn "Edge2 VPN Peer certificate"
	expires-on "Thu Nov 14 11:20:48 2019"
	key-size 256
	key-type gost2012
	}

Экспорт сертификатов и ключей на устройство Edge2	admin@Edge1:~$ pki export certificate Edge2-cert to scp://admin@203.0.113.2/home/admin/
Импорт экспортированных сертификатов и ключей на устройстве Edge2. (Имя файла export-archive.9451.tar.gz может различаться и определяется на этапе экспорта сертификатов)	admin@Edge2:~$ pki import from /home/admin/export-archive.9451.tar.gz

Для настройки Edge1 в межфилиальном режиме VPN с использованием TLS необходимо выполнить следующие действия в режиме настройки:

Пример 2.7 – Edge1 – Настройка OpenVPN – межфилиальный режим с использованием TLS

Действие	Команда
Создание узла конфигурации vtun0	[edit] admin@Edge1# set interfaces openvpn vtun0
Назначение локального IP-адреса туннеля VPN	[edit] admin@Edge1# set interfaces openvpn vtun0 local-address 192.168.100.1
Установка режима OpenVPN	[edit] admin@Edge1# set interfaces openvpn vtun0 mode site-to-site
Установка удаленного IP-адреса туннеля VPN	[edit] admin@Edge1# set interfaces openvpn vtun0 remote-address 192.168.100.2
Указание физического IP-адреса удаленного устройства	[edit] admin@Edge1# set interfaces openvpn vtun0 remote-host 203.0.113.2
Указание транспортного протокола	[edit] admin@Edge1# set interfaces openvpn vtun0 protocol tcp-passive
Установка роли данного оконечного устройства	[edit] admin@Edge1# set interfaces openvpn vtun0 tls role passive
Указание имени сертификата в модуле PKI локального узла	[edit] admin@Edge1# set interfaces openvpn vtun0 tls x509-cert Edge1-cert
Фиксация изменений	[edit] admin@Edge1# commit

Вывод настройки OpenVPN	[edit]
	admin@Edge1# show interfaces openvpn vtun0
	local-address 192.168.100.1
	mode site-to-site
	protocol tcp-passive
	remote-address 192.168.100.2
	remote-host 203.0.113.2
	tls {
	role passive
	x509-cert Edge1-cert
	}

Следует отметить, что приведенная настройка аналогична приведенной в предыдущем разделе за исключением того, что параметр **shared-secret-key** заменен на параметр **tls**.

Для настройки Edge2 в межфилиальном режиме VPN с использованием TLS необходимо выполнить следующие шаги в режиме настройки:

Пример 2.8 – Edge2 – Настройка OpenVPN – межфилиальный режим с использованием TLS

Действие	Команда
Создание узла конфигурации vtun0	[edit] admin@Edge2# set interfaces openvpn vtun0
Назначение локального IP-адреса туннеля VPN	[edit] admin@Edge2# set interfaces openvpn vtun0 local-address 192.168.100.2
Установка режима OpenVPN	[edit] admin@Edge2# set interfaces openvpn vtun0 mode site-to-site
Установка удаленного IP-адреса туннеля VPN	[edit] admin@Edge2# set interfaces openvpn vtun0 remote-address 192.168.100.1
Указание физического IP-адреса удаленного устройства	[edit] admin@Edge2# set interfaces openvpn vtun0 remote-host 203.0.113.1
Указание транспортного протокола	[edit] admin@Edge1# set interfaces openvpn vtun0 protocol tcp-active
Установка роли данного оконечного устройства	[edit] admin@Edge2# set interfaces openvpn vtun0 tls role active
Указание имени сертификата в модуле PKI локального узла	[edit] admin@Edge2# set interfaces openvpn vtun0 tls x509-cert Edge2-cert
Фиксация изменений	[edit] admin@Edge2# commit

Настройка аналогична приведенной в предыдущем примере за исключением того, что указан параметр tls.

8.3 Клиент-серверный режим

При построении VPN удаленного доступа одно оконечное устройство OpenVPN исполняет роль сервера. Удаленные пользователи OpenVPN являются клиентами, которые подключаются к серверу и устанавливают туннели VPN. Такой тип подключения приведен на рисунке 3.

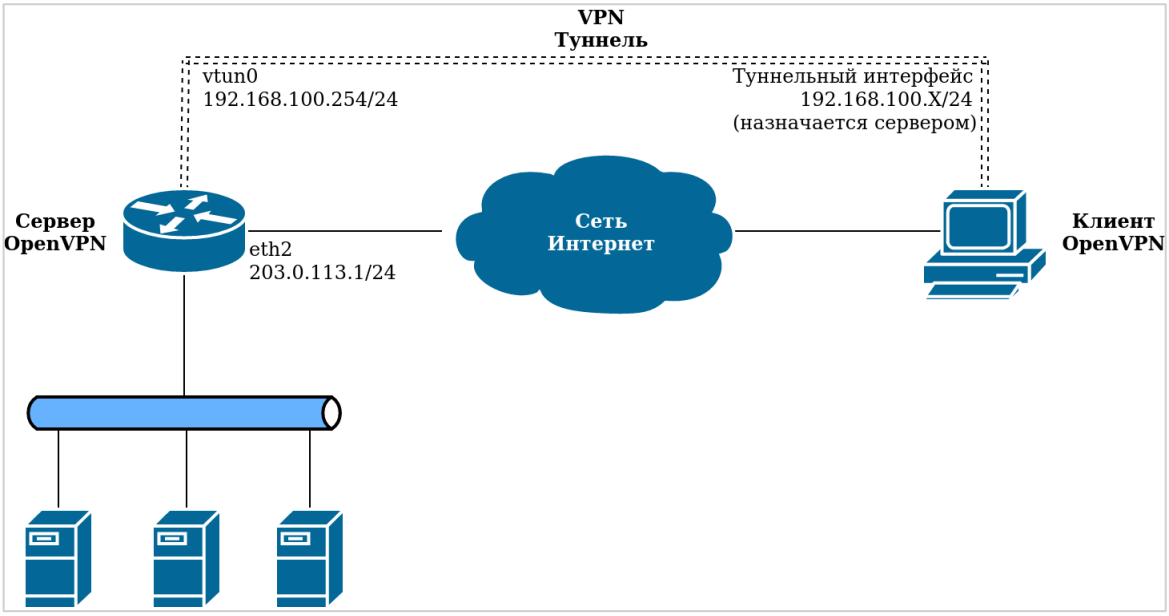


Рисунок 3 – Клиент-серверный режим

Следует отметить, что при использовании клиент-серверного режима OpenVPN требуется использование TLS, при этом сервер исполняет пассивную роль, а клиенты – активную. Таким образом, при использовании этого режима не требуется указывать параметр **tls role**. В следующем примере предполагается, что устройство Edge1 является сервером, а устройство Edge2 является клиентом. Следует отметить, что клиентом OpenVPN может выступать любое другое устройство.

Для того чтобы настроить Edge1 для работы в клиент-серверном режиме с использованием TLS, необходимо выполнить следующие действия в режиме настройки. В этом примере:

- параметр **mode** позволяет указать, что данное устройство будет работать в серверном режиме (**server**);
- параметр **server subnet** позволяет указать подсеть 192.168.100.0/24, из которой сервер будет назначать клиентам туннельные IP-адреса. Также этот параметр определяет туннельный IP-адрес сервера (адрес vtun0 на сервере) 192.168.100.254;
- значение для параметра **remote-host** не устанавливается, так как инициировать подключения к серверу будут клиенты.

Пример 2.9 – Edge1 - Настройки OpenVPN - клиент-серверный режим с использованием TLS (сервер)

Действие	Команда
Создание настройки vtun0	`[edit]` `admin@Edge1# set interfaces openvpn vtun0`
Установка режима OpenVPN	`[edit]` `admin@Edge1# set interfaces openvpn vtun0 mode server`
Указание физического адреса, на котором будут приниматься входящие подключения	`[edit]` `admin@Edge1# set interfaces openvpn vtun0 local-host 203.0.113.1`

Действие	Команда
Установка подсети для туннеля OpenVPN	[edit] admin@Edge1# set interfaces openvpn vtun0 server subnet 192.168.100.0/24
Указание имени сертификата в модуле PKI локального узла	[edit] admin@Edge1# set interfaces openvpn vtun0 tls x509-cert Edge1-cert
Указание транспортного протокола	[edit] admin@Edge1# set interfaces openvpn vtun0 protocol tcp-passive
Фиксация изменений	[edit] admin@Edge1# commit

Вывод настройки OpenVPN	[edit]
	admin@Edge1# show interfaces openvpn vtun0
	local-host 203.0.113.1
	mode server
	protocol tcp-passive
	server {
	subnet 192.168.100.0/24
	}
	tls {
	x509-cert Edge1-cert
	}

Для настройки Edge2 для работы в клиент-серверном режиме с использованием TLS необходимо выполнить следующие действия в режиме настройки. В этом примере:

- Edge2 работает в режиме клиента, и для того чтобы клиент имел возможность подключаться к серверу, его IP-адрес должен быть указан в настройке клиента при помощи параметра **remote-host**;
- после того как туннель установлен, IP-адрес туннеля устройства Edge2 (то есть адрес vtun0 на Edge2) будет назначен устройством Edge1 из подсети 192.168.100.0/24.

Пример 2.10 – Edge2 – Настройка OpenVPN – клиент-серверный режим с использованием TLS (клиент)

Действие	Команда
Создание узла конфигурации vtun0	[edit] admin@Edge2# set interfaces openvpn vtun0
Установка режима OpenVPN	[edit] admin@Edge2# set interfaces openvpn vtun0 mode client

Действие	Команда
Указание физического IP-адреса удаленного устройства	[edit] admin@Edge2# set interfaces openvpn vtun0 remote-host 203.0.113.1
Указание транспортного протокола	[edit] admin@Edge1# set interfaces openvpn vtun0 protocol tcp-active
Указание имени сертификата в модуле PKI локального устройства	[edit] admin@Edge2# set interfaces openvpn vtun0 tls x509-cert Edge2-cert
Фиксация изменений	[edit] admin@Edge2# commit

Вывод настройки OpenVPN	[edit]
	admin@Edge2# show interfaces openvpn vtun0
	mode client
	protocol tcp-active
	remote-host 203.0.113.1
	tls {
	x509-cert Edge2-cert
	}

8.4 Настройка межсетевого экрана

Применение правил межсетевого экрана к туннельному интерфейсу OpenVPN аналогично применению правил к интерфейсам другого типа.

Для настройки межсетевого экрана на устройстве Edge1 необходимо выполнить следующие действия в режиме настройки.

Пример 2.11 – Настройка правил межсетевого экрана для интерфейса OpenVPN

Действие	Команда
Создание узла конфигурации vtun0	[edit] admin@Edge1# set interfaces openvpn vtun0
Установка правила межсетевого экрана для входящего трафика на интерфейсе vtun0. (Политика фильтрации FW-vpn-outbound должна быть ранее определена в блоке police firewall)	[edit] admin@Edge1# set interfaces openvpn vtun0 policy out firewall FW-vpn-outbound
Фиксация изменений	[edit] admin@Edge1# commit
Вывод настройки OpenVPN	[edit] admin@Edge1# show interfaces

Действие	Команда

	openvpn vtun0
	...
	  policy {
	  out {
	  firewall FW-vpn-outbound
	  }
	  }
	...

9 ПРИМЕРЫ НАСТРОЙКИ С ИСПОЛЬЗОВАНИЕМ ДОПОЛНИТЕЛЬНЫХ ПАРАМЕТРОВ

В предыдущем разделе были представлены основные варианты использования OpenVPN, а также действия, которые требуются для их настройки. В данном разделе представлены дополнительные параметры, которые могут быть полезны для создания более сложных решений.

В этом разделе рассматриваются следующие вопросы:

- Транспортный протокол (межфилиальный режим, режим клиента, режим сервера);
- Разделение трафика (межфилиальный режим, режим клиента, режим сервера);
- Множественные удаленные оконечные устройства (режим клиента);
- Клиент-серверная топология (режим сервера);
- Настройки клиента (режим сервера);
- Неподдерживаемые параметры OpenVPN.

9.1 Транспортный протокол (межфилиальный режим, режим клиента, режим сервера)

По умолчанию OpenVPN использует протокол UDP в качестве транспортного протокола. Так как UDP является протоколом без установления соединения, любая сторона может инициировать туннель VPN, отправив пакет UDP на порт 1194 (по умолчанию) другому оконечному устройству. Также в качестве транспортного протокола OpenVPN может использовать протокол TCP. Однако, в том случае если используется TCP, одно оконечное устройство должно работать в пассивном режиме (**passive**) (то есть, в режиме ожидания входящих соединений TCP), а другое оконечное устройство должно работать в активном режиме (**active**) (то есть инициировать соединения TCP на порт TCP пассивного узла).

С этой точки зрения каждый протокол имеет свои преимущества. Например, при использовании межсетевого экранирования или технологии преобразования сетевых адресов (NAT) между двумя оконечными устройствами предпочтительнее использование протокола TCP.

Однако, в условиях потерь сетевых пакетов, повторы передачи TCP на уровне туннеля могут пересекаться с повторами отдельных потоков TCP внутри туннеля VPN; таким образом, в этом случае предпочтительнее использование протокола UDP.

Соответствующие параметры настройки приведены в примере 3.1 и описаны ниже

ПРИМЕЧАНИЕ. Использование протокола UDP в качестве транспортного протокола совместимо не со всеми режимами шифрования. Перед использованием необходимо ознакомиться с описанием команды конфигурационного режима:
interfaces openvpn <vtunx> encryption <алгоритм>

Пример 3.1 – Настройка параметра типа протокола

```
interfaces {
   openvpn <интерфейс> {
      protocol <протокол>
      local-host <ip-адрес>
      local-port <порт>
      remote-port <порт>
   }
}
```

protocol: корректные значения для данного параметра: **udp**, **tcp-active**, и **tcp-passive**, а также аналогичные им для IPv6 – **udp6**, **tcp6-active**, **tcp6-passive**. В том случае если значение для параметра **protocol** явно не определено или указано значение **udp** или **udp6**, используется протокол UDP. С другой стороны, если используется протокол TCP, необходимо учитывать следующие требования:

- как было указано выше, при использовании протокола TCP одно из оконечных устройств должно функционировать в пассивном режиме, а другое – в активном режиме;
- на активном устройстве (**tcp-active, tcp6-active**) должен быть установлен параметр **remote-host**, для того чтобы данное устройство имело возможность устанавливать соединения;
- если на устройстве, работающем в пассивном режиме (**tcp-passive, tcp6-passive**), установлен параметр **remote-host**, то только клиентское устройство с указанным IP-адресом сможет устанавливать соединения TCP с данным пассивным устройством;
- в том случае если протокол TCP используется при построении VPN удаленного доступа (клиент-серверном режиме), клиент должен работать в активном режиме (**tcp-active, tcp6-active**), а сервер – в пассивном режиме (**tcp-passive, tcp6-passive**);
- при использовании протокола TCP в комбинации с TLS, активный/пассивный режим для протоколов TCP и TLS должен совпадать. Другими словами, активное устройство (**tcp-active, tcp6-active**) также должно быть активным для протокола TLS (аналогичное справедливо и для пассивного устройства). Следует отметить, что данное ограничение не накладывается OpenVPN, но строго рекомендуется.

local-host: в качестве значения для данного параметра может быть указан IP-адрес или сетевой интерфейс данного оконечного устройства. В том случае если параметр **local-host** установлен, процесс OpenVPN будет принимать только подключения, приходящие на указанный IP-адрес. Это справедливо как для протокола UDP, так и для протокола TCP. В том случае если параметр **local-host** не установлен, OpenVPN принимает входящие подключения на всех интерфейсах. Данный параметр может быть использован для:

- оконечного устройства, являющегося сервером при использовании клиент-серверного режима;
- любого оконечного устройства при использовании протокола UDP в межфилиальном режиме;
- пассивного оконечного устройства (**tcp-passive, tcp6-passive**) при использовании протокола TCP в межфилиальном режиме.

local-port: данный параметр определяет номер порта UDP или TCP, на котором OpenVPN будет принимать входящие подключения. В том случае если параметр не установлен, OpenVPN принимает подключения на порту 1194. Данный параметр может быть установлен для:

- оконечного устройства, являющегося сервером при использовании клиент-серверного режима;
- любого оконечного устройства при использовании протокола UDP в межфилиальном режиме;
- пассивного оконечного устройства (**tcp-passive, tcp6-passive**) при использовании протокола TCP в межфилиальном режиме.

remote-port: данный параметр определяет номер сетевого порта UDP или TCP на другом оконечном устройстве, к которому OpenVPN инициирует подключения. Другими словами, это номер сетевого порта, на котором другое оконечное устройство принимает входящие подключения. В том случае если значение для данного параметра не установлено, OpenVPN инициирует подключения на сетевой порт, заданный по умолчанию (1194), на удаленном оконечном устройстве. Следует отметить, что если параметр **remote-port** установлен, его значение должно совпадать со значением параметра **local-port**, установленном на другом устройстве. Данный параметр может быть использован для:

- оконечного устройства, являющегося клиентом, при использовании клиент-серверного режима;
- любого оконечного устройства при использовании протокола UDP в межфилиальном режиме;
- активного устройства (**tcp-active, tcp6-active**) при использовании протокола TCP в межфилиальном режиме.

9.2 Разделение трафика (межфилиальный режим, режим клиента, режим сервера)

При установлении туннеля OpenVPN между двумя оконечными устройствами по умолчанию через туннель маршрутизируется только трафик VPN. Остальной сетевой трафик, например, сетевые пакеты, отправляемые на другие устройства посредством сети Интернет, продолжает маршрутизироваться с использованием маршрута по умолчанию. Данная технология называется разделением трафика (или разделением туннеля, split tunneling), так как позволяет разделить трафик на безопасный и небезопасный.

Разделение трафика позволяет повысить эффективность, так как трафик, не относящийся к VPN (например, интернет-трафик), отправляется по обычному маршруту, при этом к трафику применяются только локальные настройки и политики. Стоит учитывать, что политики и ограничения, установленные на второй точке туннеля (например, центральный офис организации) к этому трафику не применяются. При отключении разделения трафика происходит замена маршрута по умолчанию на туннельный адрес сервера VPN: весь исходящий трафик по умолчанию будет туннелироваться на сервер VPN и далее. Такой подход несколько замедляет обычную работу в сети Интернет, однако позволяет применять политики к исходящему трафику в одной центральной точке – на сервере VPN.

Для того чтобы отключить разделение трафика, следует использовать настройку, которая приведена в примере 3.3.

Пример 3.3 – Настройка параметров, относящихся к разделению трафика

```
interfaces {
   openvpn интерфейс {
      replace-default-route {
         local
      }
   }
```

```
}
```

replace-default-route: данный параметр позволяет указать OpenVPN, что маршрут по умолчанию должен быть заменен маршрутом через туннель VPN, то есть разделение трафика должно быть отключено. При установке данного параметра автоматически выполняются команды маршрутизации, которые позволяют направить весь сетевой трафик через туннель VPN:

- создается статический маршрут к внешнему адресу, на котором удаленный узел OpenVPN принимает подключения, через исходный маршрут по умолчанию;
- удаляется исходный маршрут по умолчанию;
- устанавливается новый маршрут по умолчанию через туннельный адрес удаленного узла OpenVPN.

Следует отметить, что при установке данного параметра получаемый результат будет зависеть от режима работы OpenVPN, в котором функционирует оконечное устройство:

- в том случае если оконечное устройство работает в межфилиальном режиме или режиме клиента, установка параметра **replace-default-route** заменит маршрут по умолчанию для данного оконечного устройства маршрутом через туннель VPN;
- если оконечное устройство функционирует в режиме сервера, установка параметра **replace-default-route** приведет к тому, что на клиентских устройствах, которые подключаются к данному серверу, будет заменен маршрут по умолчанию.

local: данный параметр внутри дерева настройки **replace-default-route** должен быть установлен тогда и только тогда, когда оба оконечных устройства подключены напрямую, то есть находятся в одной и той же подсети. В том случае если установлен данный параметр, при выполнении команд маршрутизации пропускается шаг 1, то есть не создается статический маршрут к внешнему адресу удаленного узла OpenVPN через исходный маршрут по умолчанию.

Так как туннельный интерфейс OpenVPN является маршрутизируемым, то для изменения поведения, принятого по умолчанию, могут быть добавлены статические маршруты вне зависимости от того, заменяется ли маршрут по умолчанию.

9.3 Множественные удаленные оконечные устройства (режим клиента)

В клиент-серверном режиме параметр **remote-host** должен быть указан на клиентских оконечных устройствах для того, чтобы они могли инициировать сеансы VPN. В некоторых случаях требуется указать список серверов — в случае отказа одного из серверов, клиент может подключиться к другому. Для того чтобы указать список серверов, следует указать множественные узлы настройки **remote-host**.

Для того чтобы настроить несколько оконечных устройств на Edge2, необходимо выполнить следующие действия в режиме настройки.

Пример 3.4 – Edge2 - Настройка нескольких оконечных устройств OpenVPN

Действие	Команда
Создание узла конфигурации vtun0	`[edit]` `admin@Edge2# set interfaces openvpn vtun0`
Команды дополнительной настройки	`...`

Действие	Команда
Указание физического IP-адреса первого удаленного устройства	[edit] admin@Edge1# set interfaces openvpn vtun0 remote-host 203.0.113.11
Указание физического IP-адреса второго удаленного устройства	[edit] admin@Edge1# set interfaces openvpn vtun0 remote-host 203.0.113.12
Указание физического IP-адреса третьего удаленного устройства	[edit] admin@Edge1# set interfaces openvpn vtun0 remote-host 203.0.113.13
Установка правила межсетевого экрана для входящего трафика на интерфейсе vtun0	[edit] admin@Edge2# set interfaces openvpn vtun0 policy in firewall name rules-in
Команды дополнительной настройки	...
Фиксация изменений	[edit] admin@Edge2# commit
Вывод настройки OpenVPN	[edit] admin@Edge2# show interfaces openvpn vtun0 ... remote-host 203.0.113.11 remote-host 203.0.113.12 remote-host 203.0.113.13 ...

В том случае если указаны несколько записей, клиент инициирует подключение к первому устройству **remote-host** в списке. В том случае если первое устройство не работает, клиент попытается инициировать подключение ко второму устройству и так далее.

Следует отметить, что множественные записи **remote-host** могут быть также указаны для межфилиального режима. Однако, так как два оконечных устройства обычно зафиксированы в этом режиме, использование данной возможности не имеет смысла в большинстве случаев.

9.4 Клиент-серверная топология (режим сервера)

В режиме удаленного доступа (клиент-серверном режиме) могут быть использованы две различные клиент-серверные топологии: «подсеть» (subnet) и «точка-точка» (point-to-point), как показано в примере 3.5.

Пример 3.5 – Настройка параметров, относящихся к топологии

```
interfaces {
   openvpn интерфейс  {
      server {
         topology [subnet|point-to-point]
```

```
            }
        }
    }
```

Параметр **topology** в основном определяет то, каким образом настроен интерфейс туннеля, каким образом выделяются адреса:

- **subnet**: данная топология совместима с клиентами под управлением ОС Windows и принята по умолчанию, в том случае если значение для параметра **topology** явно не указано. При использовании топологии такого типа будут функционировать протоколы маршрутизации, использующие широковещательные рассылки. Однако при использовании данной топологии не обеспечивается изоляция клиентов; то есть клиенты досягаемы друг для друга;
- **point-to-point**: данная топология не совместима с клиентами под управлением ОС Windows, а также протоколы маршрутизации, использующие широковещательные рассылки, не будут функционировать при использовании данной топологии. Данная технология обеспечивает изоляцию клиентов.

9.5 Настройки клиента (режим сервера)

Клиент-серверный режим может быть использован для организации туннеля между маршрутизаторами, что позволяет организовать защищенное взаимодействие между удаленными локальными сетями, расположенными за сервером и клиентом. Такой тип подключения может быть использован наряду с межфилиальным режимом OpenVPN для объединения в единую сеть нескольких филиалов предприятия. Данная топология приведена в примере 4.

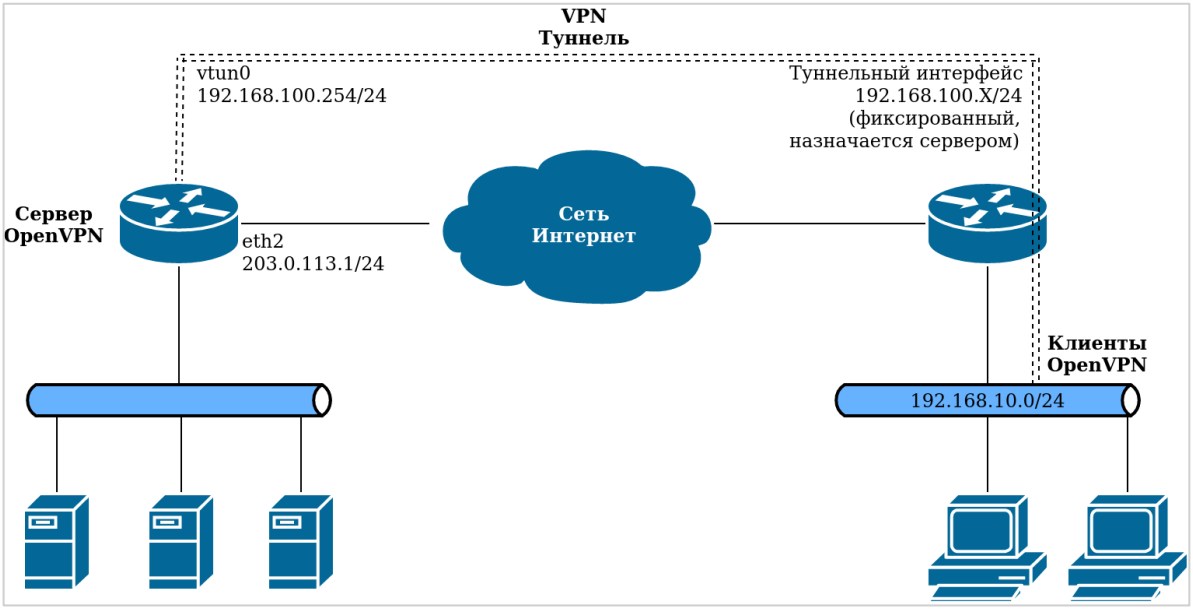


Рисунок 4 – Межфилиальное соединение VPN на базе клиент-серверного режима OpenVPN

В этом случае может быть полезно выделить фиксированный IP-адрес каждому клиенту. В том случае если за клиентом расположена частная сеть, серверу OpenVPN необходимо знать, что трафик, предназначенный для этой частной сети, необходимо маршрутизировать на конкретное клиентское устройство. Другими словами, существуют настройки, предназначенные для конкретного клиента, они могут быть установлены с использованием параметров, приведенных в примере 3.6.

Пример 3.6 – Настройка параметров, относящихся к клиентам

```
interfaces {
   openvpn <интерфейс> {
      server {
         client <имя_клиента> {
            ip <ipv4-адрес>
            subnet <подсеть>
         }
      }
   }
}
```

- **client**: данный параметр определяет имя клиента; данное имя соответствует общему имени («common name») в сертификате клиента. Когда клиент инициирует сессию VPN, сервер проверяет имя, указанное в сертификате, и применяет настройки, предназначенные для данного клиента (если они существуют);
- **ip**: данный параметр определяет фиксированный IP-адрес, который будет назначен конкретному клиенту;
- **subnet**: данный параметр определяет частную подсеть, расположенную за клиентом. Процесс OpenVPN будет маршрутизировать трафик, предназначенный для этой подсети, через указанного клиента. Следует отметить, что данный параметр информирует сервер OpenVPN, на какое клиентское устройство следует маршрутизировать трафик для этой подсети. Однако до того, как сервер OpenVPN будет принимать решение по маршрутизации, данный сетевой трафик должен быть маршрутизирован на туннельный интерфейс для того, чтобы он был обработан сервером OpenVPN. По этой причине должен быть отдельно добавлен статический маршрут для направления данного трафика на туннельный интерфейс.

В вышеприведенном примере сервер Edge1 может быть настроен с указанием IP-адреса и подсети клиента Edge2 (следует отметить, что также должен быть добавлен статический маршрут к подсети Edge2).

Для настройки данного варианта подключения, необходимо выполнить следующие действия в режиме настройки.

Пример 3.7 – Edge1 – Настройка OpenVPN – межфилиальное подключение с использованием статического ключа

Действие	Команда
Создание узла конфигурации vtun0	`[edit]` `admin@Edge1# set interfaces openvpn vtun0`
Команды дополнительной настройки	`...`
Создание конфигурационного узла сервера	`[edit]` `admin@Edge1# set interfaces openvpn vtun0 server`
Команды дополнительной настройки	`...`
Создание узла конфигурации клиента	`[edit]`

Действие	Команда
Edge2	admin@Edge1# set interfaces openvpn vtun0 server client Edge2
Установка подсети клиента	[edit] admin@Edge1# set interfaces openvpn vtun0 server client Edge2 subnet 192.168.10.0/24
Указание IP-адреса клиента	[edit] admin@Edge1# set interfaces openvpn vtun0 server client Edge2 ip 192.168.100.100
Команды дополнительной настройки	...
Фиксация изменений	[edit] admin@Edge1# commit

Вывод настройки OpenVPN	[edit]
	admin@Edge1# show interfaces openvpn vtun0
	...
	server {
	  ...
	  client Edge2 {
	  ip 192.168.100.100
	  subnet 192.168.10.0/24
	  }
	  ...
	}
	...

Для настройки статического маршрута, который позволит обеспечить доступ к удаленной подсети через туннель OpenVPN, необходимо выполнить следующие действия в режиме настройки.

Пример 3.8 – Настройка статического маршрута на узле Edge1

Действие	Команда
Создание статического маршрута для получения доступа к удаленной подсети через туннель OpenVPN	[edit] admin@Edge1# set protocols static interface-route 192.168.10.0/24 next-hop-interface vtun0
Фиксация изменений	[edit] admin@Edge1# commit
Вывод настройки статических маршрутов	[edit] admin@Edge1# show protocols static interface-route 192.168.10.0/24 {

Действие	Команда
	next-hop-interface vtun0 }

9.6 Неподдерживаемые параметры OpenVPN

OpenVPN имеет более двухсот параметров, не все из которых поддерживаются в настройке Изделия В то же время администратору в некоторых случаях могут потребоваться параметры OpenVPN, не поддерживаемые при настройке Изделия. Для таких случаев в системе существует атрибут настройки **openvpn-option**; этот атрибут позволяет определить любой параметр OpenVPN, см. пример 3.9.

Пример 3.9 – Атрибут настройки "openvpn-option"

```
interfaces {
   openvpn <интерфейс> {
      openvpn-option <опции>
   }
}
```

Текстовое значение атрибута **openvpn-option** передается напрямую (без какой-либо проверки допустимости) процессу OpenVPN во время запуска OpenVPN так, как если бы данное текстовое значение было введено пользователем в командной строке. Следовательно, одновременно могут быть введены несколько параметров, как показано ниже.

Для настройки, соответствующей данному примеру, необходимо выполнить следующие действия в режиме настройки.

Пример 3.10 – Ввод нескольких параметров OpenVPN при помощи «openvpn-option»

Действие	Команда
Создание узла конфигурации vtun0	[edit] admin@Edge1# set interfaces openvpn vtun0
Команды дополнительной настройки	...
Установка требуемых параметров OpenVPN	[edit] admin@Edge1# set interfaces openvpn vtun0 openvpn-option "--tun-mtu 1420 --verb 5"
Команды дополнительной настройки	...
Фиксация изменений	[edit] admin@Edge1# commit
Вывод настройки OpenVPN	[edit] admin@Edge1# show interfaces openvpn vtun0 ... openvpn-option "--tun-mtu 1420 --

Действие	Команда
	verb 5" ...

Для данного параметра не выполняется никакая проверка допустимости; таким образом, при его использовании следует убедиться, что параметр OpenVPN, а также его значения (в том случае если оно указано) корректны. Более того, так как многие параметры OpenVPN конфликтуют с остальными, следует также убедиться в том, что указанные параметры не конфликтуют с теми, которые используются в настройке. Также некоторые параметры OpenVPN требуют согласования между двумя оконечными устройствами, например, значение должно равняться 0 на одной стороне и 1 на другой. Необходимо убедиться, что значения согласованы.

10 Команды OpenVPN

В данном разделе приведены следующие команды:

Команды настройки	
Общие команды OpenVPN	
interfaces openvpn <vtunx>	Определение интерфейса OpenVPN.
interfaces openvpn <vtunx> bond-group <bondx>	Добавление интерфейса OpenVPN в группу агрегирования.
interfaces openvpn <vtunx> bridge-group [bridge <brX> | cost <стоимость> | priority <приоритет>]	Добавление интерфейса OpenVPN в мостовую группу
interfaces openvpn <vtunx> description <описание>	Текстовое описание интерфейса OpenVPN.
interfaces openvpn <vtunx> disable	Отключение интерфейса OpenVPN с сохранением настройки
interfaces openvpn <vtunx> encryption <алгоритм>	Указание алгоритма шифрования, используемого для туннеля OpenVPN.
interfaces openvpn <vtunx> hash <алгоритм>	Указание хэш-алгоритма, используемого для туннеля OpenVPN.
interfaces openvpn <vtunx> local-address <ipv4-адрес>	Назначение IP-адреса туннельному интерфейсу локального оконечного узла OpenVPN.
interfaces openvpn <vtunx> local-host <ip-адрес>	Указание локального адреса для сервиса OpenVPN.
interfaces openvpn <vtunx> local-port <порт>	Указание номера порта, на котором будут приниматься входящие подключения.
interfaces openvpn <vtunx> mode <режим>	Указание режима функционирования OpenVPN.
interfaces openvpn <vtunx> openvpn-option <параметры>	Указание дополнительных параметров OpenVPN.
interfaces openvpn <vtunx> protocol <протокол>	Указание используемого транспортного протокола.
interfaces openvpn <vtunx> remote-address <ipv4-адрес>	Назначение IP-адреса туннельного интерфейса удаленного оконечного узла OpenVPN.
interfaces openvpn <vtunx> remote-host <узел>	Указание IP-адреса или символьного имени удаленного узла OpenVPN, к которому будет производиться подключение.
interfaces openvpn <vtunx> remote-port <порт>	Указание номера порта, на который будут направляться исходящие подключения.
interfaces openvpn <vtunx> replace-default-route	Указание маршрута по умолчанию через туннель OpenVPN.
Сервер OpenVPN	
interfaces openvpn <vtunx> server	Определение режима сервера для оконечного

	узла OpenVPN.
interfaces openvpn <vtunx> server client <имя_узла>	Определение клиентского узла на данном сервере.
interfaces openvpn <vtunx> server client <имя_узла> name <имя_клиента>	Задание имени клиента, для которого будут применены персональные настройки VPN.
interfaces openvpn <vtunx> server client <имя_узла> x509-cert <сертификат>	Задание имени клиента, для которого будут применены персональные настройки VPN, путем указания сертификата.
interfaces openvpn <vtunx> server client <client-name> ip <ipv4-адрес>	Указание IP-адреса клиента.
interfaces openvpn <vtunx> server push-dns <ipv4-адрес>	Указание адреса сервера DNS, который будет отправлен всем клиентам OpenVPN.
interfaces openvpn <vtunx> server client <имя_узла> push-dns <ipv4-адрес>	Указание адреса сервера DNS, который будет отправлен указанному клиенту OpenVPN.
interfaces openvpn <vtunx> server client <имя_узла> subnet <ipv4-сеть>	Указание подсети на клиентском узле.
interfaces openvpn <vtunx> server max-connections <количество_клиентов>	Указание максимального количества клиентов, которые могут быть единовременно подключены к данному серверу.
interfaces openvpn <vtunx> server push-route <ipv4-сеть>	Передача клиентскому узлу маршрута к сети, расположенной за сервером OpenVPN.
interfaces openvpn <vtunx> server subnet <ipv4-сеть>	Указание подсети, из которой клиенту будет выделен IP-адрес.
interfaces openvpn <vtunx> server topology <топология>	Указание используемой топологии.
interfaces openvpn <vtunx> shared-secret-key <имя_файла>	Указание файла, содержащего статический ключ, который является общим для участников защищенного туннеля.
TLS	
interfaces openvpn <vtunx> tls	Определение настройки TLS (Transport Layer Security).
interfaces openvpn <vtunx> tls auth-key <ключ>	Добавление общего ключа, используемого для аутентификации при установлении TLS соединения.
interfaces openvpn <vtunx> tls dh-param-numbits <битность>	Разрядность параметров, используемых в протоколе обмена Диффи-Хеллмана.
interfaces openvpn <vtunx> tls x509-cert <имя_сертификата>	Указание сертификата данного оконечного узла.
interfaces openvpn <vtunx> tls role <роль>	Указание роли TLS данного оконечного устройства.
interfaces openvpn <vtunx> tls verify	Указание метода проверки сертификатов

<метод>	удаленных узлов.
interfaces openvpn <vtunx> tls version min <версия>	Указание минимальной версии протокола TLS.
interfaces openvpn <vtunx> tls version max <версия>	Указание максимальной версии протокола TLS.
Эксплуатационные команды	
vpn openvpn-key delete <имя_ключа>	Удаление файла статического ключа из системного хранилища.
vpn openvpn-key export <имя_ключа> to <имя_файла>	Экспорт файла, содержащего статический ключ.
vpn openvpn-key generate <имя_ключа>	Генерация файла, содержащего статический ключ.
vpn openvpn-key import <имя_ключа>	Импорт файла статического ключа в системное хранилище.
vpn openvpn-key list	Просмотр файлов статических ключей в системном хранилище.
vpn openvpn-export <vtunx>	Экспорт файлов настройки клиента.
vpn openvpn-export <vtunx> client-cert <сертификат> to <имя_файла>	Удаленный экспорт файла конфигурации клиента OpenVPN с сертификатами безопасности.
vpn openvpn-export <vtunx> to <имя_файла>	Удаленный экспорт файла конфигурации клиента OpenVPN
service openvpn restart	Сброс и перезапуск подключений OpenVPN.
service openvpn show interfaces	Вывод состояния всех интерфейсов OpenVPN.
service openvpn show interfaces <интерфейс>	Вывод детализированных сведений о состоянии интерфейса OpenVPN.
service openvpn show interfaces <интерфейс> brief	Вывод кратких сведений о состоянии интерфейса OpenVPN.
service openvpn show interfaces <интерфейс> capture	Запись данных, проходящих через интерфейс OpenVPN.
service openvpn show interfaces detail	Вывод детализированных сведений о состоянии всех интерфейсов OpenVPN в системе.
service openvpn show server-status	Вывод сведений о подключенных клиентах (в режиме сервера).
Команды для работы с СКЗИ «МагПро КриптоПакет»	
Команды для работы с СКЗИ «МагПро КриптоПакет»	Вывод сведений о действующей лицензии СКЗИ
vendor cryptocom license import key <lic_key>	Получение файла лицензии СКЗИ по лицензионному ключу

vendor cryptocom license import from <имя_файла>	Ввод файла лицензии СКЗИ
vendor cryptocom license update	Обновление лицензии
vendor cryptocom platform show	Вывод информации о платформе для формирования файла запроса лицензии.

10.1 Команды настройки

10.1.1 interfaces openvpn <vtunx>

Определение интерфейса OpenVPN.

Синтаксис

```
set interfaces openvpn <vtunx>
delete interfaces openvpn <vtunx>
show interfaces openvpn <vtunx>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

Можно определить более одного интерфейса OpenVPN, для этого следует создать соответствующее количество узлов конфигурации **interfaces openvpn**.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется на настройки интерфейса OpenVPN.

Форма **set** данной команды используется для создания интерфейса OpenVPN.

Форма **delete** используется для удаления всех настроек интерфейса OpenVPN.

Форма **show** данной команды используется для отображения настройки интерфейса OpenVPN.

10.1.2 interfaces openvpn <vtunx> bond-group <bondx>

Добавление интерфейса OpenVPN в группу агрегирования.

Синтаксис

```
set interfaces openvpn <vtunx> bond-group <bondx>
delete interfaces openvpn <vtunx> bond-group <bondx>
```

```
show interfaces openvpn <vtunx> bond-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      bond-group bondx
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

bondx

Идентификатор группы агрегирования.

Значение по умолчанию

Отсутствуют.

Указания по использованию

Эта команда используется для добавления интерфейса OpenVPN в группу агрегирования каналов. В группу агрегирования может быть добавлен интерфейс, настроенный в межфилиальном режиме.

Интерфейс OpenVPN может быть членом только одной группы агрегирования каналов, а группа агрегирования должна быть предварительно определена с помощью команды **interfaces bonding <bondx>**. Максимальное число интерфейсов, которое можно добавить в группу агрегирования, зависит от имеющихся системных ресурсов. Для большинства реализаций оно практически не ограничено.

ПРИМЕЧАНИЕ. Если интерфейс OpenVPN отключен с сохранением настройки (*interfaces openvpn <vtunx> disable)*, он не будет добавлен в группу агрегирования. В том случае если интерфейс неактивен, например, если в данный момент соединение не установлено, то он будет присутствовать в группе агрегирования.

Если интерфейс предполагается добавить в группу агрегирования, настраивать IP-адрес для него нельзя. Вместо этого настраивается IP-адрес для группы с помощью команды **interfaces bonding <bondx> address**. В связи с этим параметры **local-address** и **remote-adress** не указываются в конфигурации OpenVPN при добавлении виртуального интерфейса OpenVPN в группу агрегирования.

Конфигурация параметров local-address и remote-address осуществляется с помощью команд interfaces openvpn <vtunx> local-address <ipv4-адрес> и interfaces openvpn <vtunx> remote-address <ipv4-адрес> соответственно.

Форма **set** этой команды используется для добавления интерфейса OpenVPN в группу агрегирования каналов.

Форма **delete** этой команды используется для удаления интерфейса OpenVPN из группы агрегирования каналов.

Форма **show** этой команды используется для просмотра настройки группы агрегирования.

10.1.1 interfaces openvpn <vtunx> bridge-group [bridge <brX> | cost <стоимость> | priority <приоритет>]

Добавление интерфейса OpenVPN в мостовую группу.

Синтаксис

```
set interfaces openvpn <vtunx> bridge-group [bridge <brX>|cost <стоимость>|priority <приоритет>]

delete interfaces openvpn <vtunx> bridge-group [bridge <brX>|cost <стоимость>|priority <приоритет>]

show interfaces openvpn <vtunx> bridge-group [bridge <brX>|cost <стоимость>|priority <приоритет>]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      bridge-group {
         bridge <brX>
         cost <стоимость>
         priority <приоритет>
      }
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

brx

Включение интерфейса OpenVPN в состав мостовой группы.

стоимость

Установка стоимости пути для интерфейса OpenVPN, входящего в состав мостовой группы.

приоритет

Установка приоритета для интерфейса OpenVPN, входящего в состав мостовой группы.

Значение по умолчанию

Отсутствуют.

Указания по использованию

Команда используется для добавления интерфейса OpenVPN в мостовую группу. Данная настройка используется для объединения двух и более территориальных площадок с единой адресацией через VPN (L2 VPN).

ПРИМЕЧАНИЕ. Несмотря на изначальную простоту настройки, настоятельно не рекомендуется использование данной схемы, поскольку она может приводить к сложно диагностируемым проблемам.

Интерфейс OpenVPN может быть членом только одной мостовой группы, а мостовая группа должна быть предварительно определена с помощью команды **interfaces bridge <brx>**. В указанную мостовую группу с использованием аналогичной команды (**interfaces <тип_интерфейса> <интерфейс> bridge-group bridge <brx>**) добавляются другие интерфейсы изделия, трафик с которых необходимо передать через VPN на другие устройства.

Если интерфейс OpenVPN добавляется в мостовую группу, настраивать IP-адрес для него нельзя. Вместо этого настраивается IP-адрес для мостовой группы с помощью команды interfaces bridge <brx> address. В связи с этим параметры local-address и remote-address для режима site-to-site, а также узел конфигурации **server** для серверного режима не должны настраиваться для данного OpenVPN интерфейса.

Форма **set** этой команды используется для добавления интерфейса OpenVPN в мостовую группы.

Форма **delete** этой команды используется для удаления интерфейса OpenVPN из мостовой группы.

Форма **show** этой команды используется для просмотра настройки мостовой группы.

10.1.2 interfaces openvpn <vtunx> description <описание>

Текстовое описание интерфейса OpenVPN.

Синтаксис

```
set interfaces <openvpn vtunx> description <описание>
delete interfaces openvpn <vtunx> description
show interfaces openvpn <vtunx> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      description текст
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

описание

Мнемоническое имя или описание интерфейса OpenVPN. Максимальная длина ограничена 100 символами.

Если в описании присутствуют любые не алфавитно-цифровые символы, необходимо заключать описание либо в одинарные (*'описание'*), либо в двойные (*"описание"*) кавычки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для установки текстового описания интерфейса OpenVPN.

Форма **set** данной команды используется для установки описания.

Форма **delete** данной команды используется для удаления описания.

Форма **show** данной команды используется для отображения настройки описания.

10.1.3 interfaces openvpn <vtunx> disable

Отключение интерфейса OpenVPN с сохранением настройки.

Синтаксис

```
set interfaces openvpn <vtunx> disable
delete interfaces openvpn <vtunx> disable
show interfaces openvpn <vtunx>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      disable
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

Значение по умолчанию

Отсутствует.

Указания по использованию

Команда используется для отключения интерфейса OpenVPN без удаления настройки.

Форма **set** данной команды используется для отключения интерфейса.

Форма **delete** данной команды используется для включения интерфейса.

Форма **show** данной команды используется для отображения настройки интерфейса OpenVPN.

10.1.4 interfaces openvpn <vtunx> encryption <алгоритм>

Указание алгоритма шифрования, используемого для защиты данных, передаваемых по туннелю OpenVPN.

Синтаксис

```
set interfaces openvpn <vtunx> encryption <алгоритм>
delete interfaces openvpn <vtunx> encryption
show interfaces openvpn <vtunx> encryption
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      encryption алгоритм
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

алгоритм

Алгоритм шифрования, который используется для туннеля OpenVPN. Допустимы следующие значения:

- **bf128**: алгоритм Blowfish со 128-битным ключом в режиме CBC;
- **bf256**: алгоритм Blowfish с 256-битным ключом в режиме CBC;
- **aes128**: алгоритм AES со 128-битным ключом в режиме CBC;
- **aes192**: алгоритм AES со 192-битным ключом в режиме CBC;
- **aes256**: алгоритм AES с 256-битным ключом в режиме CBC;
- **gost89**: алгоритм ГОСТ 28147-89 в режиме CFBKM;
- **gost89-cbc**: алгоритм ГОСТ 28147-89 в режиме CBC.

Реализации с применением СКЗИ «МагПро КриптоПакет»:

- **gost89-cc**: алгоритм ГОСТ 28147-89;
- **kuznechik-ctr-acpkm-cc**: алгоритм кузнечик (ГОСТ Р 34.12-2015) в режиме CTR-ACPKM;
- **kuznechik-mgm-cc**: алгоритм Кузнечик (ГОСТ Р 34.12-2015) в режиме AEAD-MGM;
- **magma-ctr-acpkm-cc**: алгоритм Магма (ГОСТ Р 34.12-2015) в режиме CTR-ACPKM;
- **magma-mgm-cc**: алгоритм Магма (ГОСТ Р 34.12-2015) в режиме AEAD-MGM.

Значение по умолчанию

По умолчанию используется алгоритм ГОСТ 28147-89 (gost89).

Указания по использованию

Данная команда используется для настройки алгоритма шифрования, который применяется к данным, передаваемым по туннелю OpenVPN.

Режимы шифрования:

- **CBC** – режим сцепления блоков шифротекста (Cipher Block Chaining);
- **CFBKM** – режим гаммирования с обратной связью (Cipher Feed Back) с перемешиванием ключей (Key Meshing, RFC 4357);
- **CTR-ACPKM** – режим гаммирования с преобразованием ключа (CTR-ACPKM, англ. Counter Advanced Cryptographic Prolongation of Key Material), определенный ГОСТ Р 1323565.1.017-2018 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования»;
- **AEAD-MGM** – мультилинейный режим с аутентификацией Галуа (MGM, англ. Multilinear Galois Mode) – режим аутентифицированного шифрования с ассоциированными данными (AEAD, англ. Authenticated Encryption with Associated Data), определенный ГОСТ Р 1323565.1.026–2019 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, реализующие аутентифицированное шифрование».

ПРИМЕЧАНИЕ. Для использования сертифицированного ФСБ средства криптографической защиты информации «МагПро КриптоПакет» необходимо выбирать алгоритм имеющий суффикс "-cc" (например magma-mgm-cc).

ВНИМАНИЕ. При использовании шифрования с перемешиванием ключей (Key Meshing, RFC 4357) (gost-89, gost89-cc, kuznechik-ctr-acpkm-cc, magma-ctr-acpkm-cc) требуется обеспечение гарантии доставки и порядка сетевых пакетов, что в общем случае не совместимо с использованием в качестве транспорта протокола UDP.

Форма **set** данной команды используется для указания используемого алгоритма шифрования OpenVPN.

Форма **delete** данной команды используется для отмены использования текущего алгоритма шифрования и возвращения к использованию алгоритма, принятого по умолчанию.

Форма **show** данной команды используется для отображения алгоритма шифрования, используемого для данного туннеля OpenVPN.

10.1.5 interfaces openvpn <vtunx> hash <алгоритм>

Указание хэш-алгоритма, используемого для туннеля OpenVPN.

Синтаксис

```
set interfaces openvpn <vtunx> hash <алгоритм>
delete interfaces openvpn <vtunx> hash
show interfaces openvpn <vtunx> hash
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      hash алгоритм
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

алгоритм

Хэш-алгоритм, который используется для указанного туннеля OpenVPN. Поддерживаемые значения:

- **gost**: алгоритм ГОСТ 28147-89 в режиме выработки имитовставки;
- **md5**: HMAC на основе MD5 (Message Digest 5);
- **sha1**: HMAC на основе SHA-1 (Secure Hash Algorithm);
- **sha256**: HMAC на основе SHA-256;
- **sha512**: HMAC на основе SHA-512;
- **cmac**: CMAC на основе выбранного алгоритма шифрования данных;
- **kuznechik-mac**: алгоритм Кузнечик (ГОСТ Р 34.12-2015) в режиме выработки имитовставки;
- **magma-mac**: алгоритм Магма (ГОСТ Р 34.12-2015) в режиме выработки имитовставки.

Значение по умолчанию

Используется алгоритм SHA-1.

Указания по использованию

Данная команда используется для настройки хэш-алгоритма, которые применяется для данного туннеля OpenVPN. Следует учитывать, что алгоритмы:

- алгоритмы **kuznechik-mac** и **magma-mac** доступны только при использовании СКЗИ «МагПро КриптоПакет»;
- алгоритм **cmac** не доступен при использовании СКЗИ «МагПро КриптоПакет».

Данная настройка игнорируется при использовании AEAD режимов шифрования (например, magma-mgm-cc).

Допустимые формы команды:

Форма **set** данной команды используется для указания хэш-алгоритма, применяемого для указанного туннеля OpenVPN.

Форма **delete** данной команды используется для отмены использования текущего хэш-алгоритма и возвращения к использованию алгоритма, принятого по умолчанию.

Форма **show** данной команды используется для отображения хэш-алгоритма, используемого для данного туннеля OpenVPN.

10.1.6 interfaces openvpn <vtunx> local-address <ipv4-адрес>

Назначение IP-адреса туннельному интерфейсу локального оконечного узла OpenVPN.

Синтаксис

```
set interfaces openvpn <vtunx> local-address <ipv4-адрес>
delete interfaces openvpn <vtunx> local-address
show interfaces openvpn <vtunx> local-address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      local-address ipv4-адрес
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

ipv4-адрес

Обязательный. IPv4-адрес.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для настройки туннельного IP-адреса локального оконечного узла OpenVPN. Может быть определен только один адрес. Установка данного параметра требуется при использовании межфилиального режима и не требуется при использовании клиент-серверного режима.

При настройке межфилиального режима и добавлении интерфейса OpenVPN настраивать IP-адрес для него нельзя. Вместо этого настраивается IP-адрес для группы с помощью команды **interfaces bonding <bondx> address**. В связи с этим значение для параметра **local-address** не указывается в конфигурации OpenVPN при добавлении виртуального интерфейса OpenVPN в группу агрегирования.

Форма **set** используется для установки туннельного IP-адреса локального оконечного узла туннеля OpenVPN.

Форма **delete** данной команды используется для удаления туннельного IP-адреса локального оконечного узла туннеля OpenVPN.

Форма **show** данной команды используется для отображения туннельного IP-адреса локального оконечного узла туннеля OpenVPN.

10.1.7 interfaces openvpn <vtunx> local-host <ip-адрес>

Указание физического IP-адреса, на котором будут приниматься входящие подключения.

Синтаксис

```
set interfaces openvpn <vtunx> local-host <ip-адрес>
delete interfaces openvpn <vtunx> local-host
show interfaces openvpn <vtunx> local-host
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      local-host ip-адрес
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

ip-адрес

Необязательный. IP-адрес локального физического интерфейса, на котором принимаются входящие подключения. В том случае если значение для данного параметра явно не указано, подключения принимаются на всех интерфейсах. Допустимо использование как IPv4, так и IPv6 адресов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания локального IP-адреса, на котором принимаются подключения. Значение для данного параметра может быть указано для устройства, являющегося сервером при использовании клиент-серверного режима, а также для устройства, работающего в пассивном режиме (**tcp-passive, tcp6-passive**) при использовании протокола TCP в межфилиальном режиме. В качестве значения для данного параметра может быть указан IP-адрес любого интерфейса данного устройства. В том случае если значение для данного параметра установлено, процесс OpenVPN будет принимать подключения, приходящие только на указанный IP-адрес, это справедливо как для протокола UDP, так и для протокола TCP. В том случае если значение явно не указано, OpenVPN принимает входящие подключения на всех интерфейсах.

Форма **set** данной команды используется для указания IP-адреса, на котором принимаются входящие подключения.

Форма **delete** данной команды используется для удаления указанного локального IP-адреса, на котором принимаются входящие подключения.

Форма **show** данной команды используется для отображения локального IP-адреса, на котором принимаются подключения.

10.1.8 interfaces openvpn <vtunx> local-port <порт>

Указание номера порта, на котором будут приниматься входящие подключения.

Синтаксис

```
set interfaces openvpn <vtunx> local-port <порт>
delete interfaces openvpn <vtunx> local-port
show interfaces openvpn <vtunx> local-port
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      local-port порт
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

порт

Необязательный. Номер порта, на котором будут приниматься входящие подключения. По умолчанию используется номер порта 1194.

Значение по умолчанию

По умолчанию установлено значение 1194.

Указания по использованию

Данная команда используется для настройки локального порта UDP или TCP, на котором будут приниматься входящие подключения. Значение для данного параметра может быть указано для устройства, являющегося сервером в клиент-серверном режиме, а также для устройства, работающего в пассивном режиме (**tcp-passive**) при использовании протокола TCP в межфилиальном режиме.

Форма **set** данной команды позволяется указать локальный порт, на котором принимаются входящие подключения.

Форма **delete** данной команды позволяет удалить указанный локальный порт, на котором принимаются входящие подключения, и восстановить значение, принятое по умолчанию.

Форма **show** данной команды используется для отображения локального сетевого порта, на котором принимаются входящие подключения.

10.1.9 interfaces openvpn <vtunx> mode <режим>

Указание режима функционирования интерфейса OpenVPN.

Синтаксис

```
set interfaces openvpn vtun<vtunx>  mode <режим>
delete interfaces openvpn <vtunx> mode
```

```
show interfaces openvpn <vtunx> mode
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      mode [client|server|site-to-site]
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

режим

Обязательный. Режим работы интерфейса OpenVPN. Поддерживаемые значения:

- **client**: оконечное устройство будет функционировать в качестве клиента OpenVPN для туннеля OpenVPN с клиент-серверной топологией;
- **server**: оконечное устройство будет функционировать в качестве сервера OpenVPN для туннеля OpenVPN с клиент-серверной топологией;
- **site-to-site**: устройство будет являться оконечным узлом туннеля OpenVPN с межфилиальной топологией.

ПРИМЕЧАНИЕ. При использовании СКЗИ «МагПро КриптоПакет» (параметр **encryption *-cc**) в Изделии по умолчанию не поддерживается работа в режиме **client.** Для настройки защищенного соединения между несколькими Изделиями с применением СКЗИ «МагПро КриптоПакет», рекомендуется использовать режим функционирования **site-to-site**. Для огранизации точки подключения к защищенной сети клиентских устройств, таких как ПК, мобильные устройства и т. д. в Изделии необходимо использовать режим функционирования **server.** При этом на пользовательских устройствах должна быть установлена клиентская лицензия для использования в качестве VPN-клиента для Изделия.

При необходимости функционирования СКЗИ «МагПро КриптоПакет» в режиме **client** обратитесь в техническую поддержку производителя.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания режима работы интерфейса OpenVPN.

Форма **set** данной команды позволяет указать режим работы интерфейса OpenVPN.

Форма **delete** используется для удаления установленного режима работы интерфейса OpenVPN.

Форма **show** данной команды используется для отображения режима работы интерфейса OpenVPN.

10.1.10 interfaces openvpn <vtunx> openvpn-option <параметры>

Указание дополнительных параметров OpenVPN.

Синтаксис

```
set interfaces openvpn <vtunx> openvpn-option <параметры>
delete interfaces openvpn <vtunx> openvpn-option
show interfaces openvpn <vtunx> openvpn-option
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    openvpn vtunx {
        openvpn-option текст
    }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

параметры

Строка параметров, которые будут переданы процессу OpenVPN.

ПРИМЕЧАНИЕ. Список параметров должен быть заключен в кавычки, а каждый параметр в списке должен начинаться с двух знаков минус, при этом параметры должны быть разделены пробелом. Например, при применении дополнительных параметров **ping** со значением **10** и **float** на интерфейсе **vtun1**, выполняемая команда будет выглядеть так: **set interfaces openvpn vtun1 openvpn-options "--float --ping 10"**

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания дополнительных параметров OpenVPN, которые не могут быть настроены при помощи команд настройки OpenVPN, предоставляемых интерфейсом командной строки Изделия. Так как процесс OpenVPN имеет более двухсот команд, только основные из них могут быть настроены при помощи команд Изделия. Данная команда обеспечивает возможность использования всех остальных параметров, доступных в OpenVPN. Более подробная информация о параметрах OpenVPN приведена на сайте http://openvpn.net/.

Форма **set** данной команды позволяет использовать дополнительные параметры OpenVPN.

Форма **delete** данной команды используется для удаления дополнительных параметров OpenVPN.

Форма **show** данной команды используется для отображения дополнительных параметров OpenVPN.

10.1.11 interfaces openvpn <vtunx> protocol <протокол>

Указание транспортного протокола OpenVPN.

Синтаксис

```
set interfaces openvpn <vtunx> protocol <протокол>

delete interfaces openvpn <vtunx> protocol

show interfaces openvpn <vtunx> protocol
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    openvpn vtunx {
          protocol    [tcp-active|tcp-passive|udp|tcp6-active|tcp6-passive|udp6]
    }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

протокол

Транспортный протокол, используемый OpenVPN. Поддерживаемые значения:

- **tcp6-active**: транспортный протокол TCP – активная роль. При использовании протокола IPv6;
- **tcp6-passive**: транспортный протокол TCP – пассивная роль. При использовании протокола IPv6;
- **udp6**: транспортный протокол UDP. При использовании протокола IPv6;
- **tcp-active**: транспортный протокол TCP – активная роль;
- **tcp-passive**: транспортный протокол TCP – пассивная роль;
- **udp**: транспортный протокол UDP. Используется по умолчанию.

Значение по умолчанию

По умолчанию установлено значение **udp**.

Указания по использованию

Данная команда используется для указания транспортного протокола OpenVPN.

ПРИМЕЧАНИЕ. При использовании шифрования с перемешиванием ключей (Key Meshing, RFC 4357) (gost-89, gost89-cc, kuznechik-ctr-acpkm-cc, magma-ctr-acpkm-cc)

требуется обеспечение гарантии доставки и порядка сетевых пакетов, что в общем случае не совместимо с использованием в качестве транспорта протокола UDP.

Форма **set** данной команды используется для указания используемого транспортного протокола OpenVPN.

Форма **delete** используется для удаления настройки используемого OpenVPN транспортного протокола и восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки транспортного протокола, используемого OpenVPN.

10.1.12 interfaces openvpn <vtunx> remote-address <ipv4-адрес>

Назначение IP-адреса туннельного интерфейса удаленного оконечного узла OpenVPN.

Синтаксис

```
set interfaces openvpn <vtunx> remote-address <ipv4-адрес>
delete interfaces openvpn <vtunx> remote-address
show interfaces openvpn <vtunx> remote-address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      remote-address ipv4-адрес
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

ipv4-адрес

Обязательный. Туннельный IP-адрес удаленного оконечного узла OpenVPN.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для настройки туннельного IP-адреса удаленного оконечного узла туннеля OpenVPN. Может быть определен только один адрес. Установка данного параметра требуется при использовании межфилиального режима и не требуется при использовании клиент-серверного режима.

Форма **set** данной команды используется для указания туннельного IP-адреса удаленного оконечного узла туннеля OpenVPN.

Форма **delete** данной команды используется для удаления туннельного IP-адреса удаленного оконечного узла туннеля OpenVPN.

Форма **show** данной команды используется для отображения туннельного IP-адреса удаленного оконечного узла туннеля OpenVPN.

10.1.13 interfaces openvpn <vtunx> remote-host <узел>

Указание IP-адреса или символьного имени удаленного узла OpenVPN, к которому будет производиться подключение.

Синтаксис

```
set interfaces openvpn <vtunx> remote-host <узел>
delete interfaces openvpn <vtunx> remote-host
show interfaces openvpn <vtunx> remote-host
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      remote-host узел
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

узел

Удаленный IP-адрес или символьное имя (hostname) узла, к которому будет производиться подключение.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для настройки удаленного IP-адреса или имени узла (hostname), к которому осуществляются подключения. Значение для данного параметра необходимо указать при использовании клиент-серверного режима в настройке клиентского устройства, для того чтобы указать ему сервер, к которому будет осуществляться подключение. Также значение для данного параметра требуется указать в межфилиальном режиме для обоих оконечных узлов.

Форма **set** данной команды используется для установления IP-адреса узла, к которому осуществляются подключения.

Форма **delete** данной команды используется для удаления указанного удаленного IP-адреса узла, к которому осуществляются подключения.

Форма **show** данной команды позволяет отобразить удаленный IP-адрес узла, к которому осуществляются подключения.

10.1.14 interfaces openvpn <vtunx> remote-port <порт>

Указание номера порта, на который будут направляться исходящие подключения.

Синтаксис

```
set interfaces openvpn <vtunx> remote-port <порт>
delete interfaces openvpn <vtunx> remote-port
show interfaces openvpn <vtunx> remote-port
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      remote-port порт
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

порт

Необязательный. Номер порта, на который будут направляться исходящие подключения. По умолчанию используется номер порта 1194.

Значение по умолчанию

По умолчанию установлено значение 1194.

Указания по использованию

Данная команда позволяет настроить удаленный порт UDP или TCP, на который будут направляться исходящие подключения. Значение для данного параметра может быть указано для устройства, являющегося клиентом, в клиент-серверном режиме, а также для устройства, работающего в активном режиме (**tcp-active**) при использовании протокола TCP в межфилиальном режиме. Следует отметить, что в том случае если параметр **remote-port** установлен, его значение должно совпадать со значением параметра **local-port** установленном на удаленном узле.

Форма **set** данной команды используется для указания удаленного порта UDP или TCP, на который будут направляться исходящие подключения.

Форма **delete** данной команды позволяет удалить указанный порт UDP или TCP, на который направляются исходящие подключения.

Форма **show** данной команды используется для отображения номера порта UDP или TCP, на который направляются исходящие подключения.

10.1.15 interfaces openvpn <vtunx> replace-default-route

Указание маршрута по умолчанию через туннель OpenVPN.

Синтаксис

```
set interfaces openvpn <vtunx> replace-default-route [local]
delete interfaces openvpn <vtunx> replace-default-route
show interfaces openvpn <vtunx> replace-default-route
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      replace-default-route {
         local
      }
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

local

Необязательный. Данный параметр должен быть установлен тогда и только тогда, когда оба оконечных устройства подключены напрямую, то есть находятся в одной и той же подсети.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать, что маршрут по умолчанию должен быть заменен маршрутом через туннель VPN, то есть разделение трафика должно быть отключено. Следует отметить, что при установке данного параметра, получаемый результат будет зависеть от режима работы OpenVPN, в котором функционирует оконечное устройство:

- в том случае если оконечное устройство работает в межфилиальном режиме или режиме клиента, установка параметра **replace-default-route** заменит маршрут по умолчанию для данного оконечного устройства маршрутом через туннель VPN;
- если оконечное устройство функционирует в режиме сервера, установка параметра **replace-default-route** приведет к тому, что на клиентских устройствах, которые подключаются к данному серверу будет заменен маршрут по умолчанию.

При установке данного параметра автоматически выполняются команды маршрутизации, которые позволяют направить весь сетевой трафик через туннель VPN:

1) создается статический маршрут к внешнему адресу, на котором удаленный узел OpenVPN принимает подключения, через исходный маршрут по умолчанию;
2) удаляется исходный маршрут по умолчанию;
3) устанавливается новый маршрут по умолчанию через туннельный адрес удаленного

узла OpenVPN.

Параметр **local** необходимо устанавливать в том случае, если оба сервера OpenVPN находятся в одной и той же подсети. В том случае если установлен данный параметр, при выполнении команд маршрутизации пропускается шаг 1, то есть не создается статический маршрут к внешнему адресу удаленного узла OpenVPN через исходный маршрут по умолчанию.

Форма **set** данной команды используется для замены маршрута по умолчанию на маршрут через туннель OpenVPN.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

10.2 Сервер OpenVPN

10.2.1 interfaces openvpn <vtunx> server

Определение режима сервера для оконечного устройства OpenVPN.

Синтаксис

```
set interfaces openvpn <vtunx> server
delete interfaces openvpn <vtunx> server
show interfaces openvpn <vtunx> server
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      server
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания того, что данный узел будет выполнять роль сервера в клиент-серверном режиме.

Форма **set** данной команды используется для создания узла конфигурации серверного режима.

Форма **delete** данной команды используется для удаления узла конфигурации серверного режима.

Форма **show** используется для отображения настройки.

10.2.2 interfaces openvpn <vtunx> server client <имя_узла>

Определение настройки клиентского узла для данного сервера.

Синтаксис

```
set interfaces openvpn <vtunx> server client <имя_узла>
delete interfaces openvpn <vtunx> server client <имя_узла>
show interfaces openvpn <vtunx> server client <имя_узла>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      server {
         client имя_узла
      }
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN.

имя_узла

Обязательный. Имя клиентского узла.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данный узел конфигурации позволяет задать персональные настройки отдельному клиенту VPN, такие как IP адрес, DNS сервер, статические маршруты и др. Идентификация клиента VPN производится по имени (Common Name) в его персональном сертификате, предоставляемом клиентом на этапе подключения к изделию. Соответствующие персональные настройки будут применены к клиенту VPN, если имя клиента совпадает с заданным в конфигурации изделия. Имя клиента может быть задано следующими параметрами конфигурации:

- **set interfaces openvpn <vtunx> server client <имя_узла>** - рассматриваемый узел конфигурации. Изначально для сопоставления в качестве имени клиента используется имя рассматриваемого узла - **<имя_узла>**;
- **set interfaces openvpn <vtunx> server client <имя_узла> x509-cert <сертификат>** - при задании указанного параметра, для сопоставления в качестве имени клиента будет использоваться значение Common Name указанного сертификата, хранящегося в хранилище Изделия;

- **set interfaces openvpn <vtunx> server client <имя_узла> name <имя>** - при задании указанного параметра, для сопоставления в качестве имени клиента будет использоваться специально заданное этим параметром имя клиента.

Формы выполнения команды:

Форма **set** данной команды используется для создания узла конфигурации клиента.

Форма **delete** данной команды используется для удаления узла конфигурации клиента.

Форма **show** используется для отображения настройки.

10.2.3 interfaces openvpn <vtunx> server client <имя_узла> name <имя_клиента>

Задание имени клиента, для которого будут применены персональные настройки VPN.

Синтаксис

```
set interfaces openvpn <vtunx> server client <имя_узла> name <имя_клиента>
delete interfaces openvpn <vtunx> server client <имя_узла> name
show interfaces openvpn <vtunx> server client <имя_узла> name
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      server {
         client имя_узла {
            name имя_клиента
         }
      }
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN.

имя_узла

Обязательный. Имя клиентского узла.

имя_клиента

Имя клиента, для которого должны быть применены персональные настройки.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет определить имя клиента, к которому будут применены настройки, определенные в текущем узле конфигурации **interfaces openvpn <vtunx> server client <имя_узла>.** Данная настройка имеет приоритет и переопределяет значения, заданные узлами **interfaces openvpn <vtunx> server client <имя_узла>** и **interfaces openvpn <vtunx> server client <имя_узла> x509-cert**.

Форма **set** данной команды используется для создания узла конфигурации клиента.

Форма **delete** данной команды используется для удаления узла конфигурации клиента.

Форма **show** используется для отображения настройки.

10.2.4 interfaces openvpn <vtunx> server client <имя_узла> x509-cert <сертификат>

Задание имени клиента, для которого будут применены персональные настройки VPN.

Синтаксис

```
set interfaces openvpn <vtunx> server client <имя_узла> x509-cert
<сертификат>
delete interfaces openvpn <vtunx> server client <имя_узла> x509-
cert
show interfaces openvpn <vtunx> server client <имя_узла> x509-cert
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      server {
         client имя_узла {
            x509-cert сертификат
         }
      }
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN.

имя_узла

Обязательный. Имя клиентского узла.

сертификат

Имя узла конфигурации **pki ca <имя_УЦ> certificate <имя_сертификата>**.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет определить имя клиента, к которому будут применены настройки, определенные в текущем узле конфигурации **interfaces openvpn <vtunx> server client <имя_узла>.** При задании данного узла конфигурации для определения имени клиента используется значение Common Name из соответствующего сертификата из хранилища изделия. Данная настройка переопределяет значение, заданное узлом **interfaces openvpn <vtunx> server client <имя_узла>**. Если же имя клиента уже задано с использованием параметра конфигурации **interfaces openvpn <vtunx> server client <имя_узла> name <имя_клиента>**, рассматриваемая настройка будет проигнорирована.

Форма **set** данной команды используется для создания узла конфигурации клиента.

Форма **delete** данной команды используется для удаления узла конфигурации клиента.

Форма **show** используется для отображения настройки.

10.2.5 interfaces openvpn <vtunx> server client <client-name> ip <ipv4-адрес>

Указание IP-адреса клиента при использовании клиент-серверной топологии.

Синтаксис

```
set interfaces openvpn <vtunx> server client <имя_узла> ip ipv4-
<адрес>
delete interfaces openvpn <vtunx> server client <имя_узла> ip
show interfaces openvpn <vtunx> server client <имя_узла> ip
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      server {
         client имя_узла {
            ip ipv4-адрес
         }
      }
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN.

имя_узла

Обязательный. Имя клиентского узла.

ipv4-адрес

IP-адрес, который будет назначен клиенту.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет при использовании клиент-серверной топологии указать IP-адрес, который будет назначен указанному клиентскому узлу. После применения конфигурации произойдет автоматический перезапуск сервера OpenVPN и переустановление всех ранее установленных клиентских подключений. После перезапуска сервера клиентам, имеющим данный параметр, назначается IP-адрес согласно указанного параметра. Остальным клиентам IP-адрес назначается случайным образом из пула свободных IP-адресов.

Форма **set** данной команды используется для указания IP-адреса, который назначается клиентскому узлу.

Форма **delete** данной команды используется для удаления указанного IP-адреса.

Форма **show** данной команды используется для отображения указанного IP-адреса.

10.2.6 interfaces openvpn <vtunx> server push-dns <ipv4-адрес>

Указание адреса сервера DNS, который будет отправлен всем клиентам OpenVPN.

Синтаксис

```
set interfaces openvpn <vtunx> server push-dns <ipv4-адрес>
delete interfaces openvpn <vtunx> server push-dns
show interfaces openvpn <vtunx> server push-dns
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      server {
         push-dns ipv4-адрес
      }
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

ipv4-адрес

IP-адрес сервера DNS, который будет отправлен всем клиентам OpenVPN.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указывать адрес сервера DNS, который будет отправлен всем клиентам OpenVPN.

Форма **set** данной команды используется для указания IP-адреса сервера DNS, который назначается всем клиентам OpenVPN.

Форма **delete** данной команды используется для удаления указанного IP-адреса сервера DNS.

Форма **show** данной команды используется для отображения указанного IP-адреса сервера DNS.

10.2.7 interfaces openvpn <vtunx> server client <имя_узла> push-dns <ipv4-адрес>

Указание адреса сервера DNS, который будет отправлен указанному клиенту OpenVPN.

Синтаксис

```
set interfaces openvpn <vtunx> server client <имя_узла> push-dns <ipv4-адрес>
delete interfaces openvpn <vtunx> server client <имя_узла>
show interfaces openvpn <vtunx> server client <имя_узла>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    openvpn vtunx {
        server {
            client имя_узла {
                push-dns ipv4-адрес
            }
        }
    }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

имя_узла

Обязательный. Имя клиентского узла.

ipv4-адрес

IP-адрес сервера DNS, который будет отправлен указанному клиенту OpenVPN.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указывать адрес сервера DNS, который будет отправлен указанному клиенту OpenVPN.

Форма **set** данной команды используется для указания IP-адреса сервера DNS, который назначается указанному клиенту OpenVPN.

Форма **delete** данной команды используется для удаления указанного IP-адреса сервера DNS.

Форма **show** данной команды используется для отображения указанного IP-адреса сервера DNS.

10.2.8 interfaces openvpn <vtunx> server client <имя_узла> subnet <ipv4-сеть>

Указание подсети на клиентском узле при использовании клиент-серверной топологии.

Синтаксис

```
set interfaces openvpn <vtunx> server client <имя_узла> subnet <ipv4-сеть>
delete interfaces openvpn <vtunx> server client <имя_узла> subnet
show interfaces openvpn <vtunx> server client <имя_узла> subnet
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    openvpn vtunx {
        server {
            client имя_узла {
                subnet ipv4-сеть
            }
        }
    }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

имя_узла

Обязательный. Имя клиентского узла.

Когда клиент инициирует сессию VPN, сервер проверяет имя сертификата и применяет настройки, предназначенные для данного клиента (в том случае если они существуют).

ipv4-сеть

Множественный узел. Подсеть, расположенная за клиентским узлом.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать частную подсеть, расположенную за клиентским узлом. При необходимости можно указать несколько подсетей, расположенных за клиентским узлом, для этого следует создать соответствующее количество узлов конфигурации **subnet**. Процесс OpenVPN будет маршрутизировать трафик, предназначенный для данной подсети, через указанного клиента.

Изменения в персональных настройках клиентских подключений не приводят к перезапуску сервера OpenVPN, эти изменения не действуют для ранее установленных клиентских подключений и вступают в силу только после перезапуска клиентского подключения. Команда **service openvpn restart** позволяет при необходимости принудительно перезапустить все клиентские подключения.

ПРИМЕЧАНИЕ. Следует отметить, что данный параметр информирует сервер OpenVPN, на какое клиентское устройство следует маршрутизировать трафик для этой подсети. Однако до того, как сервер OpenVPN будет принимать решение по маршрутизации, данный сетевой трафик должен быть маршрутизирован на туннельный интерфейс, для того чтобы он был обработан сервером OpenVPN. По этой причине также должен быть отдельно добавлен статический маршрут для направления данного трафика на туннельный интерфейс.

Форма **set** данной команды используется для указания подсети.

Форма **delete** данной команды используется для удаления настройки подсети.

Форма **show** данной команды используется для отображения настройки подсети.

10.2.9 interfaces openvpn <vtunx> server max-connections <количество_клиентов>

Указание максимального количества клиентов, которые могут быть единовременно подключены к данному серверу.

Синтаксис

```
set interfaces openvpn <vtunx> server max-connections <количество_клиентов>

delete interfaces openvpn <vtunx> server max-connections

show interfaces openvpn <vtunx> server max-connections
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      server {
         max-connections количество_клиентов
      }
```

```
    }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

количество_клиентов

Максимальное количество клиентов, которые могут быть единовременно подключены к данному серверу.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется на стороне сервера при использовании клиент-серверной топологии и позволяет указать максимальное количество клиентов, которые могут быть единовременно подключены к данному серверу. Этот параметр может быть полезен для распределения нагрузки при использовании нескольких серверов OpenVPN.

Форма **set** данной команды используется для указания максимального количества единовременных клиентских подключений.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

10.2.10 interfaces openvpn <vtunx> server push-route <ipv4-сеть>

Передача клиентскому узлу маршрута к сети, расположенной за сервером OpenVPN.

Синтаксис

```
set interfaces openvpn <vtunx> server push-route <ipv4-сеть>
delete interfaces openvpn <vtunx> server push-route
show interfaces openvpn <vtunx> server push-route
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      server {
         push-route ipv4-сеть
      }
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

ipv4-сеть

Множественный узел. Подсеть, расположенная за сервером OpenVPN, маршрут к которой будет автоматически передаваться клиентам OpenVPN при подключении.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется на серверной стороне при использовании клиент-серверной топологии и позволяет передавать клиентам OpenVPN маршрут к подсети, расположенной за сервером OpenVPN.

При подключении клиента сервер OpenVPN передает ему маршрут к указанной подсети, после чего этот маршрут будет автоматически добавлен в таблицу маршрутизации на стороне клиента.

Для того чтобы указать несколько подсетей, создайте соответствующее количество узлов **push-route**.

Форма **set** данной команды используется для указания подсети, маршрут к которой будет передаваться клиентам OpenVPN.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

10.2.11 interfaces openvpn <vtunx> server subnet <ipv4-сеть>

Указание подсети, из которой клиенту будет выделен IP-адрес.

Синтаксис

```
set interfaces openvpn <vtunx> server subnet <ipv4-сеть>
delete interfaces openvpn <vtunx> server subnet
show interfaces openvpn <vtunx> server subnet
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      server {
         subnet ipv4-сеть
      }
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

ipv4-сеть

Подсеть, из которой клиенту будут выделяться IP-адреса.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется на серверной стороне при использовании клиент-серверной топологии и позволяет указать подсеть, из которой удаленные клиенты будут получать IP-адреса.

Данная команда используется для указания подсети, из которой удаленным клиентам будут выделяться IP-адреса.

Форма **set** данной команды используется для указания подсети.

Форма **delete** данной команды используется для удаления настройки подсети.

Форма **show** данной команды используется для отображения настройки подсети.

10.2.12 interfaces openvpn <vtunx> server topology <топология>

Указание используемой топологии в клиент-серверном режиме.

Синтаксис

```
set interfaces openvpn <vtunx> server topology <топология>
delete interfaces openvpn <vtunx> server topology
show interfaces openvpn <vtunx> server topology
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      server {
         topology [point-to-point|subnet]
      }
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

топология

Топология, используемая в клиент-серверном режиме. Поддерживаются следующие значения:

- **point-to-point**: Данная топология обеспечивает "изоляцию клиентов" (то есть, клиенты недоступны друг для друга), но она не совместима с клиентами под управлением ОС Windows, а также при использовании данной топологии не будут работать протоколы маршрутизации, использующие широковещательные рассылки.
- **subnet**: Данная топология совместима с клиентами под управлением ОС Windows и установлена по умолчанию, в том случае если значение для данного параметра явно не указано. Протоколы маршрутизации, использующие широковещательные рассылки, совместимы с данной топологией. Однако данная топология не обеспечивает "изоляции клиентов" (то есть, клиенты досягаемы друг для друга).

Значение по умолчанию

По умолчанию установлено значение **subnet**.

Указания по использованию

Данная команда используется для указания топологии сети, которая будет использоваться в клиент-серверном режиме.

Форма **set** данной команды используется для указания топологии.

Форма **delete** данной команды используется для удаления настройки топологии.

Форма **show** данной команды используется для отображения настройки топологии.

10.2.13 interfaces openvpn <vtunx> shared-secret-key <имя_файла>

Указание файла, содержащего статический ключ, который является общим для участников защищенного туннеля.

Синтаксис

```
set interfaces openvpn <vtunx> shared-secret-key <имя_файла>
delete interfaces openvpn <vtunx> shared-secret-key
show interfaces openvpn <vtunx> shared-secret-key
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      shared-secret-key текст
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

имя_ключа

Имя ключа, которое получается в результате генерации или импорта файла статического ключа соответствующими командами эксплуатационного режима. При использовании

механизма шифрования со статическим ключом, данный ключ должен быть предварительно передан на устройство, с которым устанавливается OpenVPN соединение.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания имени статического ключа, общего с удаленным оконечным узлом туннеля. Данный метод шифрования может использоваться только в межфилиальной топологии (**mode site-to-site**).

ПРИМЕЧАНИЕ. Механизм шифрования со статическим ключем несовместим с ГОСТ алгоритмами, соответственно, при их использовании возможно осуществление шифрования только используя механизм TLS.

Форма **set** данной команды используется для задания имени статического ключа, используемого при установлении защищенного соединения.

Форма **delete** данной команды используется для удаления настройки статического ключа.

Форма **show** данной команды используется для отображения настройки статического ключа.

10.3 TLS

10.3.1 interfaces openvpn <vtunx> tls

Определение настройки TLS (Transport Layer Security).

Синтаксис

```
set interfaces openvpn <vtunx> tls
delete interfaces openvpn <vtunx> tls
show interfaces openvpn <vtunx> tls
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      tls {
      }
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для определения настройки TLS (Transport Layer Security).

Форма **set** данной команды используется для создания узла конфигурации TLS.

Форма **delete** данной команды используется для удаления узла конфигурации TLS.

Форма **show** данной команды используется для отображения настройки TLS.

10.3.2 interfaces openvpn <vtunx> tls auth-key <ключ>

Добавление общего ключа, используемого для аутентификации при установлении TLS соединения.

Синтаксис

```
set interfaces openvpn <vtunx> tls auth-key <ключ>
delete interfaces openvpn <vtunx> tls auth-key
show interfaces openvpn <vtunx> tls auth-key
```

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      tls {
         auth-key <ключ>
      }
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

ключ

Имя общего ключа, находящегося в системном хранилище и используемого для аутентификации при уставновлении TLS соединения.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данный параметр используется для защиты от атак типа "отказ в обслуживании", поскольку перед установлением TLS соединения, производится дополнительная проверка подлинности инициатора соединения. Для проверки подлинности используется статический ключ, сгенерированный командой **vpn openvpn-key generate <имя_ключа>**.

После генерации данный ключ должен быть передан всем на все устройства, участвующие в OpenVPN соединении, и добавлен в их конфигурацию. В случае Numa Edge, общий ключ импортируется в системное хранилище командой **vpn openvpn-key import <имя_ключа> to <путь>**.

Форма **set** данной команды используется для указания разрядности параметров обмена.

Форма **delete** данной команды используется для удаления разрядности параметров обмена и использования значения по умолчанию.

Форма **show** используется для отображения настройки.

10.3.3 interfaces openvpn <vtunx> tls dh-param-numbits <битность>

Разрядность параметров, используемых в протоколе обмена Диффи-Хеллмана.

Синтаксис

```
set interfaces openvpn <vtunx> tls dh-param-numbits <битность>
delete interfaces openvpn <vtunx> tls dh-param-numbits
show interfaces openvpn <vtunx> tls dh-param-numbits
```

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      tls {
         dh-param-numbits <битность>
      }
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

битность

Необязательный. Задание разрядности групп Диффи-Хеллмана, используемых для ключевого обмена. Значение должно лежать в диапазоне от 1024 до 2048.

Значение по умолчанию

По умолчанию установлено значение 2048.

Указания по использованию

Для получения двумя сторонами общего секретного ключа, используя ненадежный канал связи, используется протокол Диффи-Хеллмана. Полученный ключ в дальнейшем применяется для шифрования/расшифровки сообщений, используя симметричные алгоритмы. Надежность ключевого обмена зависит от разрядности используемых групп (простых чисел) с помощью которых получается общий ключ.

Форма **set** данной команды используется для указания разрядности параметров обмена.

Форма **delete** данной команды используется для удаления разрядности параметров обмена и использования значения по умолчанию.

Форма **show** используется для отображения настройки.

10.3.4 interfaces openvpn <vtunx> tls x509-cert <имя_сертификата>

Указание имени сертификата локального оконечного узла OpenVPN.

Синтаксис

```
set interfaces openvpn <vtunx> tls x509-cert <имя_сертификата>
delete interfaces openvpn <vtunx> tls x509-cert
show interfaces openvpn <vtunx> tls x509-cert
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      tls {
         x509-cert текст
      }
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

имя_сертификата

Сертификат локального оконечного узла.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать имя сертификата локального оконечного узла. Указание значения для данного параметра является обязательным, если используется режим TLS.

Форма **set** данной команды используется для указания имени сертификата локального оконечного узла.

Форма **delete** данной команды используется для удаления настройки имени сертификата локального оконечного узла.

Форма **show** данной команды используется для отображения настройки.

10.3.5 interfaces openvpn <vtunx> tls role <роль>

Указание роли TLS данного оконечного устройства.

Синтаксис

```
set interfaces openvpn <vtunx> tls role <роль>
delete interfaces openvpn <vtunx> tls role
show interfaces openvpn <vtunx> tls role
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      tls {
         role [active|passive]
      }
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

роль

Роль TLS данного оконечного устройства. Поддерживаемые значения:

- **active**: оконечное устройство выполняет активную роль;
- **passive**: оконечное устройство выполняет пассивную роль.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания роли TLS, которую исполняет оконечное устройство. Применима только для режима site-to-site.

Форма **set** данной команды используется для указания роли TLS, которую исполняет оконечное устройство.

Форма **delete** данной команды используется для удаления роли TLS.

Форма **show** используется для отображения настройки.

10.3.6 interfaces openvpn <vtunx> tls verify <метод>

Указание метода проверки сертификатов удаленных узлов.

Синтаксис

```
set interfaces openvpn <vtunx> tls verify <метод>
delete interfaces openvpn <vtunx> tls verify
show interfaces openvpn <vtunx> tls verify
```

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      tls {
         verify <метод>
      }
   }
```

```
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

метод

Указание метода проверки сертификатов удаленных узлов. Поддерживаемые значения:

- **scvp**: проверять действительность сертификатов удаленных узлов посредством протокола SCVP (Server-based Certificate Validation Protocol) согласно политике, определённой RFC 5280, секция 6;
- **crl**: проверять действительность сертификатов удаленных узлов посредством CRL (certificate revocation list).

Значение по умолчанию

По умолчанию используется проверка сертификатов удаленных узлов по протоколу SCVP.

Указания по использованию

Данная команда позволяет выбрать метод проверки сертификатов удаленных узлов на действительность при установлении соединения OpenVPN.

Форма **set** данной команды используется для указания метода проверки сертификатов удаленных узлов.

Форма **delete** данной команды используется для удаления настройки метода проверки сертификатов и использования значения по умолчанию.

Форма **show** используется для отображения настройки.

10.3.7 interfaces openvpn <vtunx> tls version min <версия>

Указание минимальной версии протокола TLS.

Синтаксис

```
set interfaces openvpn <vtunx> tls version min <версия>
delete interfaces openvpn <vtunx> tls version min
show interfaces openvpn <vtunx> tls version min
```

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      tls {
         version min [1.0|1.1|1.2]
      }
   }
 }
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

версия

Указание минимальной версии протокола TLS. Поддерживаемые значения:

- **1.0:** используется протокол TLS 1.0, описанный в стандарте RFC 2246;
- **1.1:** используется протокол TLS 1.1, описанный в стандарте RFC 4346;
- **1.2:** используется протокол TLS 1.2, описанный в стандарте RFC 5246.

Значение по умолчанию

Для минимальной версии протокола TLS умолчанию используется TLS 1.1.

Указания по использованию

Перед установлением зашифрованного соединения, происходит согласование используемой версии TLS. Каждая из сторон сообщает список поддерживаемых версий, среди которых выбирается наибольшая версия, поддерживаемая на каждом устройстве. Данный параметр позволяет указать минимально поддерживаемую версию.

Форма **set** данной команды используется для указания метода проверки сертификатов удаленных узлов.

Форма **delete** данной команды используется для удаления настройки метода проверки сертификатов и использования значения по умолчанию.

Форма **show** используется для отображения настройки.

ПРИМЕЧАНИЕ. Некоторые устаревшие реализации openvpn не поддерживают согласование TLS, а также используют единственную версию - TLS 1.0 Использование версии TLS 1.0 рекомендуется к использованию только для обеспечения совместимости.

10.3.8 interfaces openvpn <vtunx> tls version max <версия>

Указание максимальной версии протокола TLS

Синтаксис

```
set interfaces openvpn <vtunx> tls version max <версия>
delete interfaces openvpn <vtunx> tls version max
show interfaces openvpn <vtunx> tls version max
```

Ветвь конфигурации

```
interfaces {
   openvpn vtunx {
      tls {
         version max [1.0|1.1|1.2]
      }
   }
}
```

Параметры

vtunx

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от vtun0 до vtun9999.

метод

Указание максимальной версии протокола TLS. Поддерживаемые значения:

- **1.0:** используется протокол TLS 1.0**,** описанный в стандарте RFC 2246;
- **1.1:** используется протокол TLS 1.1, описанный в стандарте RFC 4346;
- **1.2:** используется протокол TLS 1.2, описанный в стандарте RFC 5246.

Значение по умолчанию

Отсутствует

Указания по использованию

Перед установлением зашифрованного соединения, происходит согласование используемой версии TLS. Каждая из сторон сообщает список поддерживаемых версий, среди которых выбирается наибольшая версия, поддерживаемая на каждом устройстве. Данный параметр позволяет указать максимально поддерживаемую версию.

Форма **set** данной команды используется для указания метода проверки сертификатов удаленных узлов.

Форма **delete** данной команды используется для удаления настройки метода проверки сертификатов и использования значения по умолчанию.

Форма **show** используется для отображения настройки.

10.4 Эксплуатационные команды

10.4.1 vpn openvpn-key delete <имя_ключа>

Удаление файла статического ключа из системного хранилища.

Синтаксис

```
vpn openvpn-key delete <имя_ключа>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_ключа

Обязательный. Имя файла статического ключа, который будет удален.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для удаления файла, содержащего статический ключ. Данная команда доступна только для пользователей, обладающих правами администратора. Удалять ключи, используемые в конфигурации, запрещено.

10.4.2 vpn openvpn-key export <имя_ключа> to <имя_файла>

Экспорт файла, содержащего статический ключ.

Синтаксис

```
vpn openvpn-key export <имя_ключа> to <имя_файла>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_ключа

Обязательный. Имя файла статического ключа, который находится в системном хранилище ключей.

имя_файла

Обязательный. Имя локального или удаленного файла. Задает имя для файла статического ключа, который будет создан после экспорта из системного хранилища ключей. Допустимые значения:

- **<filename>** - имя локального или удаленного файла;
- **<ftp://user@host/file>** - имя локального или удаленного файла;
- **<scp://user@host/file>** - имя локального или удаленного файла;
- **<tftp://host/file>** - имя локального или удаленного файла.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для экспорта файла, содержащего статический ключ и используемого при применении механизма безопасности с использованием предварительно распределенных общих ключей. Данная команда доступна только для пользователей, обладающих правами администратора.

ПРИМЕЧАНИЕ. При использовании данной команды будет импортирован статический общий ключ, который используется для аутентификации сторон при установлении защищённого туннельного соединения OpenVPN. В случае его компрометации злоумышленник сможет расшифровать весь трафик, зашифрованный с помощью данного ключа. Поэтому во время его передачи удаленной стороне необходимо использовать защищенные каналы.

10.4.3 vpn openvpn-key generate <имя_ключа>

Генерация файла, содержащего статический ключ.

Синтаксис

```
vpn openvpn-key generate <имя_ключа>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_файла

Обязательный. Имя файла статического ключа, который будет создан.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для создания файла, содержащего статический ключ и используемого при применении механизма безопасности с использованием предварительно распределенных общих ключей или для аутентификации TLS-соединения после соответствующей настройки. Данная команда доступна только для пользователей, обладающих правами администратора.

10.4.4 vpn openvpn-key import <имя_ключа>

Импорт файла статического ключа в системное хранилище.

Синтаксис

```
vpn openvpn-key import <имя_ключа> to <имя_файла>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_ключа

Обязательный. Имя файла статического ключа, который будет импортирован.

имя_файла

Обязательный. Имя локального или удаленного файла. Задает имя для файла статического ключа, который будет импортирован в системное хранилище ключей. Допустимые значения:

- **<filename>** - имя локального или удаленного файла;
- **<ftp://user@host/file>** - имя локального или удаленного файла;
- **<scp://user@host/file>** - имя локального или удаленного файла;
- **<tftp://host/file>** - имя локального или удаленного файла.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для импорта файла, содержащего статический ключ и используемого при применении механизма безопасности с использованием предварительно распределенных общих ключей. Данная команда доступна только для пользователей, обладающих правами администратора.

ПРИМЕЧАНИЕ. При использовании данной команды будет экспортирован статический общий ключ, который используется для аутентификации сторон при установлении защищённого туннельного соединения OpenVPN. В случае его компрометации злоумышленник сможет расшифровать весь трафик, зашифрованный с помощью данного ключа. Поэтому во время его передачи удаленной стороне необходимо использовать защищенные каналы.

10.4.5 vpn openvpn-key list

Просмотр файлов статических ключей в системном хранилище.

Синтаксис

```
vpn openvpn-key list
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для просмотра статических ключей, находящихся в системном хранилище.

10.4.6 vpn openvpn-export <vtunx>

Экспорт файлов с настройками клиента на флэш-накопитель.

Синтаксис

```
vpn openvpn-export <vtunx> client-cert <сертификат>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

vtunx

Идентификатор интерфейса OpenVPN.

сертификат

Имя сертификата клиента. Значение для данного параметра должно быть указано в том случае, если для создания сертификатов клиента и сервера используется модуль PKI системы Numa Edge.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет экспортировать файл с настройками клиента на подключенный флэш-накопитель. Данная команда может быть использована только в клиент-серверном режиме на устройстве, функционирующем в режиме сервера (**mode server**). При выполнении данной команды к устройству должен быть подключен флэш-накопитель. Монтирование и размонтирование флэш-накопителя осуществляется автоматически. Экспортируемые файлы будут помещены в каталог openvpn в корневой директории флэш-накопителя. К экспортируемым файлам относятся:

- сертификат клиента;
- сертификат удостоверяющего центра;
- секретный ключ клиента;
- список отозванных сертификатов;
- командный файл **setupvpn.js**.

Командный файл **setupvpn.js** позволяет автоматически добавить настройку клиента в приложение Numa Edge VPN, которое поставляется вместе с системой Numa Edge и представляет собой графический интерфейс для использования OpenVPN в ОС Windows.

ПРИМЕЧАНИЕ. При использовании данной команды будет экспортирован секретный ключ клиента, который должен храниться в секрете. Для доставки клиенту секретного ключа необходимо использовать только безопасные каналы.

10.4.7 vpn openvpn-export <vtunx> client-cert <сертификат> to <имя_файла>

Удаленный экспорт файла конфигурации клиента OpenVPN с сертификатами безопасности.

Синтаксис

```
vpn openvpn-export <vtunx> client-cert <сертификат> to <имя_файла>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

vtunx

Идентификатор интерфейса OpenVPN.

сертификат

Имя сертификата клиента. Значение для данного параметра должно быть указано в том случае, если для создания сертификатов клиента и сервера используется модуль PKI системы Numa Edge.

имя_файла

Имя локального или удаленного файла. Задает имя для файла конфигурации, который будет создан с возможностью указания его расположения. Допустимые значения:

- **<filename>** - имя локального или удаленного файла;
- **<ftp://user@host/file>** - имя локального или удаленного файла;
- **<scp://user@host/file>** - имя локального или удаленного файла;
- **<tftp://host/file>** - имя локального или удаленного файла.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет экспортировать файл конфигурации клиента OpenVPN с сертификатами. Данная команда может быть использована только в клиент-серверном режиме на устройстве, функционирующем в режиме сервера (**mode server**). Экспортируемые файлы будут помещены в каталог openvpn в корневой директории. К экспортируемым файлам относятся:

- сертификат клиента;
- сертификат удостоверяющего центра;
- секретный ключ клиента;
- список отозванных сертификатов;
- командный файл **setupvpn.js**.

Командный файл **setupvpn.js** позволяет автоматически добавить настройку клиента в приложение Numa Edge VPN, которое поставляется вместе с системой Numa Edge и представляет собой графический интерфейс для использования OpenVPN в ОС Windows.

ПРИМЕЧАНИЕ. При использовании данной команды будет экспортирован секретный ключ клиента, который должен храниться в секрете. Для доставки клиенту секретного ключа необходимо использовать только безопасные каналы.

10.4.8 vpn openvpn-export <vtunx> to <имя_файла>

Удаленный экспорт файла конфигурации клиента OpenVPN.

Синтаксис

```
vpn openvpn-export <vtunx> to <имя_файла>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

vtunx

Идентификатор интерфейса OpenVPN.

имя_файла

Имя локального или удаленного файла. Задает имя для файла конфигурации, который будет создан с возможностью указания его расположения. Допустимые значения:

- **<filename>** - имя локального или удаленного файла;
- **<ftp://user@host/file>** - имя локального или удаленного файла;
- **<scp://user@host/file>** - имя локального или удаленного файла;
- **<tftp://host/file>** - имя локального или удаленного файла.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет экспортировать файл конфигурации клиента OpenVPN Данная команда может быть использована только в клиент-серверном режиме на устройстве, функционирующем в режиме сервера (**mode server**). Экспортируемые файлы будут помещены в каталог openvpn в корневой директории. К экспортируемым файлам относятся:

- секретный ключ клиента;
- список отозванных сертификатов;
- командный файл **setupvpn.js**.

Командный файл **setupvpn.js** позволяет автоматически добавить настройку клиента в приложение Numa Edge VPN, которое поставляется вместе с системой Numa Edge и представляет собой графический интерфейс для использования OpenVPN в ОС Windows.

ПРИМЕЧАНИЕ. При использовании данной команды будет экспортирован секретный ключ клиента, который должен храниться в секрете. Для доставки клиенту секретного ключа необходимо использовать только безопасные каналы.

10.4.9 service openvpn restart

Сброс и перезапуск всех клиентских подключений для указанного сервера.

Синтаксис

```
service openvpn restart interface <vtunx>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

vtunx

Идентификатор интерфейса сервера OpenVPN.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для перезапуска клиентских подключений для указанного сервера OpenVPN.

Изменения в персональных настройках клиентских подключений (ветвь конфигурации **interfaces openvpn <vtunx> server client**) не приводят к перезапуску сервера OpenVPN, эти изменения не действуют для ранее установленных клиентских подключений и вступают в силу только после перезапуска клиентского подключения. Данная команда позволяет при необходимости принудительно перезапустить все клиентские подключения.

10.4.10 service openvpn show interfaces

Вывод состояния всех интерфейсов OpenVPN.

Синтаксис

```
service openvpn show interfaces
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения общих сведений о состоянии всех интерфейсов OpenVPN в системе.

Примеры

Пример 4.1 – «service openvpn show interfaces»: отображение состояния интерфейса OpenVPN

```
admin@edgevpn558:~$ service openvpn show interfaces
Interface    IP Address         State       Link   Description
vtun0        172.16.0.1/24      up          up
```

10.4.11 service openvpn show interfaces <интерфейс>

Вывод детализированных сведений о состоянии интерфейса OpenVPN.

Синтаксис

```
service openvpn show interfaces <интерфейс>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

интерфейс

Имя интерфейса OpenVPN.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для вывода детализированных сведений о состоянии интерфейса OpenVPN.

Примеры

В примере ниже приведен вывод для команды **service openvpn show interfaces** <*интерфейс*>.

Пример 4.2 – «service openvpn show interfaces vtun0»: отображение состояния интерфейса OpenVPN

```
admin@edge:~$ service openvpn show interfaces vtun0
vtun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc
pfifo_fast state UNKNOWN group default qlen 100
    link/none
    inet 172.16.0.1/24 brd 172.16.0.255 scope global vtun0
       valid_lft forever preferred_lft forever
    inet6 fe80::193a:1940:862f:b4e1/64 scope link flags 800
       valid_lft forever preferred_lft forever

    RX:   bytes     packets       errors     dropped     overrun
mcast
             0           0            0           0           0
0
    TX:   bytes     packets       errors     dropped     carrier
collisions
           380           5            0           0           0
0
```

10.4.12 service openvpn show interfaces <интерфейс> brief

Вывод кратких сведений о состоянии интерфейса OpenVPN.

Синтаксис

```
service openvpn show interfaces <интерфейс> brief
```

Режим интерфейса

Эксплуатационный режим.

Параметры

интерфейс

Имя интерфейса OpenVPN.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения кратких сведений о состоянии интерфейса OpenVPN.

Примеры

В примере приведен вывод для команды **service openvpn show interfaces** <*интерфейс*> **brief**.

Пример 4.3 – «service openvpn show interfaces vtun0 brief»: отображение состояния интерфейса OpenVPN

```
admin@edge:~$ service openvpn show interfaces vtun0 brief
Interface    IP Address          State       Link   Description
vtun0        172.16.0.1/24       up          up
```

10.4.13 service openvpn show interfaces <интерфейс> capture

Запись данных, проходящих через интерфейс OpenVPN.

Синтаксис

```
service openvpn show interfaces <интерфейс> capture
```

Режим интерфейса

Эксплуатационный режим.

Параметры

интерфейс

Имя интерфейса OpenVPN.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для записи данных, проходящих через интерфейс OpenVPN. Для прекращения записи данных следует нажать <Ctrl + C>.

Примеры

В примере приведен вывод для команды **service openvpn show interfaces <***интерфейс***> capture**.

Пример 4.4 – «service openvpn show interfaces»: запись трафика на интерфейсе OpenVPN

```
admin@edge:~$ service openvpn show interfaces vtun0 capture
Capturing traffic on vtun0 ...
```

10.4.14 service openvpn show interfaces detail

Вывод детализированных сведений о состоянии всех интерфейсов OpenVPN в системе.

Синтаксис

```
service openvpn show interfaces detail
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для отображения детализированных сведений о состоянии интерфейсов OpenVPN в системе.

Примеры

В примере приведен вывод для команды **service openvpn show interfaces detail**.

Пример 4.5 – «service openvpn show interfaces detail»: отображение детализированных сведений о состоянии интерфейсов OpenVPN в системе.

```
admin@edge:~$ service openvpn show interfaces detail
vtun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc
pfifo_fast state UNKNOWN group default qlen 100
    link/none
    inet 172.16.0.1/24 brd 172.16.0.255 scope global vtun0
       valid_lft forever preferred_lft forever
    inet6 fe80::193a:1940:862f:b4e1/64 scope link flags 800
       valid_lft forever preferred_lft forever

    RX:   bytes     packets       errors     dropped     overrun
mcast
             0           0            0           0           0
0
    TX:   bytes     packets       errors     dropped     carrier
collisions
           380           5            0           0           0
0
```

10.4.15 service openvpn show server-status

Вывод сведений о подключенных клиентах (в режиме сервера).

Синтаксис

```
service openvpn show server-status
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет вывести сведения обо всех подключенных клиентских узлах. Данная команда доступна только для устройства, являющегося сервером. Также следует отметить, что вывод для этой команды не обновляется в режиме реального времени. Выводятся сведения о клиентах, подключенных на момент вызова команды.

Примеры

В примере приведен вывод для команды **service openvpn show server-status**.

Пример 4.6 – «service openvpn show server-status»: отображение состояния сервера OpenVPN

```
admin@edge:~$ service openvpn show server-status
OpenVPN server status on vtun0 (last updated on Tue Nov 13
18:42:10 2018)


Client  Remote  IP      Tunnel  IP      TX  byte    RX  byte
Connected Since
------------------------------------------  ----------------
---------------
C01   12.12.12.1    10.0.0.5      1.4K      1.3K        Tue Nov
13 05:27:24 2018
C03   11.1.1.1      10.0.0.3      64.1K     1.7K        Tue Nov
13 05:27:05 2018
C25   15.82.82.8    10.0.0.26     38.1K     35.4K       Mon Nov
12 14:28:26 2018
```

10.5 Команды для работы с СКЗИ «МагПро КриптоПакет»

10.5.1 vendor cryptocom license

Команда ранее использовалась для вывода сведений о действующей лицензии средства криптографической защиты информации СКЗИ «МагПро КриптоПакет» вер. 3.0. Для Numa Edge с СКЗИ «МагПро КриптоПакет» вер. 4.0. команда более не используется.

10.5.2 vendor cryptocom license import key <lic_key>

Получения файла лицензии СКЗИ «МагПро КриптоПакет» вер. 3.0 по лицензионному ключу. Для Numa Edge с СКЗИ «МагПро КриптоПакет» вер. 4.0. команда более не используется.

10.5.3 vendor cryptocom license import from <имя_файла>

Ввод файла лицензии СКЗИ «МагПро КриптоПакет» вер. 4.0.

Синтаксис

```
vendor cryptocom license import from <имя_файла>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_файла

Имя локального или удаленного файла. Задает имя для файла лицензии, который будет создан с возможностью указания его расположения. Файл может быть расположен локально или удаленно и доступен по протоколам ftp, scp, tftp.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда предназначена для ручного ввода файла лицензии СКЗИ «МагПро КриптоПакет». В каждом изделии Numa Edge на производстве устанавливается уникальная лицензия СКЗИ «МагПро КриптоПакет», привязанная к аппаратной платформе. При переустановке изделия с дистрибутива на компакт-диске или сброса изделия к заводским настройкам из меню загрузки - лицензия на СКЗИ «МагПро КриптоПакет» будет утеряна. Обратитесь в службу технической поддержки производителя для получения соответствующего файла лицензии.

10.5.4 vendor cryptocom license update

Обновление лицензии СКЗИ «МагПро КриптоПакет» вер. 3.0 в ручном режиме. Для Numa Edge с СКЗИ «МагПро КриптоПакет» вер. 4.0. команда более не используется.

10.5.5 vendor cryptocom platform show

Вывод информации о платформе для формирования файла запроса лицензии.

Синтаксис

```
vendor cryptocom platform show
```

Режим интерфейса

Эксплуатационный режим.

Параметры

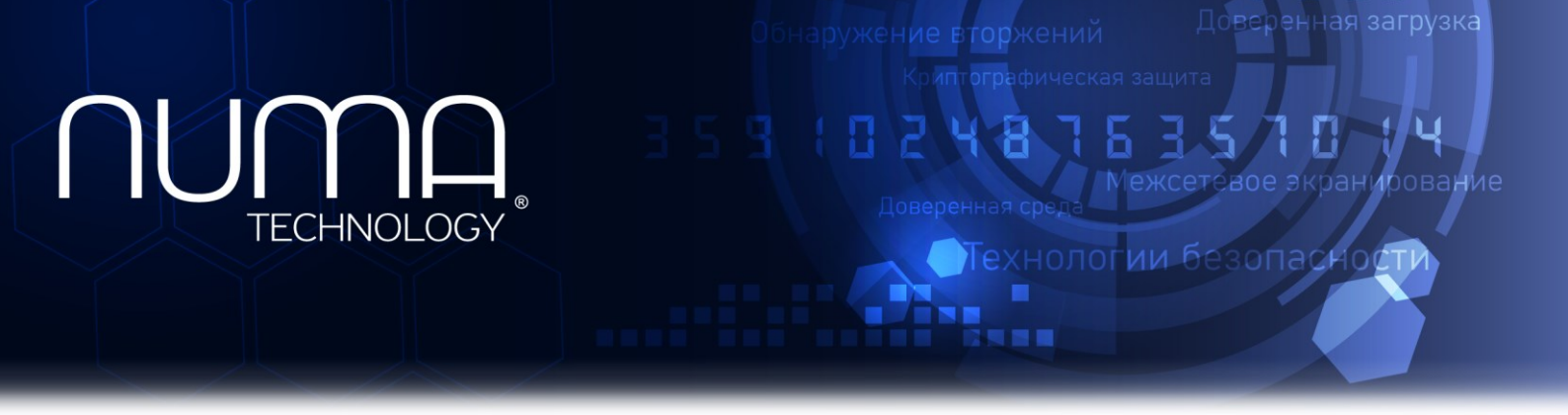
Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда предназначена для вывода на экран информации о платформе, необходимой для формирования лицензии на СКЗИ «МагПро КриптоПакет» вер. 4.0. При наличии необходимости обновления на версию изделия Numa Edge VPN требуется сохранить вывод данной команды в файл и обратиться в службу технической поддержки ООО НумаТех.



Межсетевой экран Numa Edge

Руководство администратора

Построение виртуальных частных сетей на основе набора протоколов IPSec

Листов 91

Санкт-Петербург
2021

СОДЕРЖАНИЕ

ИДЕНТИФИКАЦИЯ ДОКУМЕНТА

Название документа	Руководство администратора. Построение виртуальных частных сетей на основе набора протоколов IPSec
Версия документа	1.4
Обозначение документа	643.АМБН.00004-01 32 04
Идентификация ОО	Межсетевой экран Numa Edge
Идентификация разработчика	ООО «НумаТех»
Ключевые слова	Межсетевой экран, МЭ, IPSec

АННОТАЦИЯ ДОКУМЕНТА

Документ предназначен для ознакомления пользователя с технической информацией о настройке виртуальных частных сетей на основе набора протоколов IPSec в межсететвом экране Numa Edge и содержит сведения о примерах и командах настройки.

1. ВВЕДЕНИЕ

1.1. Межфилиальный режим IPSec

В этом документе рассматриваются следующие вопросы:

- Настройка VPN в межфилиальном режиме IPSec.
- Команды отображения состояния IPSec в межфилиальном режиме.
- Команды IPSec в межфилиальном режиме.

1.2. Настройка VPN в межфилиальном режиме IPSec

В данном разделе описано как настроить VPN с использованием межфилиального режима IPSec в системе Numa Edge.В этом разделе рассматриваются следующие вопросы:

- Обзор VPN, построенных на основе межфилиального режима IPSec.
- Фиксация изменений в настройке VPN.
- Настройка базового подключения в межфилиальном режиме.
- Аутентификация на основе схемы ЭЦП на базе RSA.
- Аутентификация на базе PKI.
- Настройка туннелей IPSec между тремя шлюзами.
- Создание подключения VPN с использованием NAT.
- Защита туннеля GRE с использованием IPSec.
- Узлы VPN, имеющие динамические IP-адреса.

1.3. Обзор VPN, построенных на основе межфилиального режима IPSec

В этом разделе рассматриваются следующие вопросы:

- Архитектура IPSec.
- Фазы IPSec: фаза 1 и фаза 2.
- Ключевой обмен IKE.
- Алгоритмы шифрования.
- Алгоритмы хеширования.
- Предварительные ключи.
- Аутентификация на основе асимметричных криптографических алгоритмов.
- Основные компоненты PKI.
- Группы Диффи-Хеллмана.
- Режимы IPSec.
- Полная безопасность пересылки.
- IPSec и QoS.

Виртуальная частная сеть (VPN) на основе IPSec - это виртуальная сеть, которая функционирует поверх сети общего доступа, но при этом является "защищенной" благодаря использованию зашифрованных туннелей между двумя и более оконечными точками. VPN позволяет обеспечить:

- Целостность данных. Целостность данных позволяет удостовериться в том, что они не были искажены или модифицированы при их передаче через сеть. Целостность данных обеспечивается за счет использования алгоритмов хеширования.
- Аутентификация. Аутентификация гарантирует, что полученные данные были отправлены заявленным отправителем, а не кем-либо, выдающим себя за него. Аутентификация также обеспечивается при помощи алгоритмов хеширования.
- Конфиденциальность. Конфиденциальность гарантирует, что данные доступны только тому, для кого они предназначены, и не могут быть скопированы или перехвачены при передаче по сети. Конфиденциальность обеспечивается при помощи шифрования.

VPN, построенная на основе IPSec, позволяет защитить данные и доступ к ресурсам сети с использованием шифрования, аутентификации и протоколов управления ключами. При корректной настройке VPN все взаимодействия безопасны, а передаваемые данные защищены от злоумышленников. Numa Edge поддерживает межфилиальный режим IPSec. Межфилиальные подключения VPN обычно устанавливаются между двумя (или более) шлюзами VPN и обеспечивают возможность взаимодействия для компьютеров пользователей, серверов и других устройств, расположенных за шлюзами. Использование межфилиального режима VPN позволяет сократить расходы на создание канала связи между офисами. Это зачастую позволяет заменить более дорогие технологии WAN, такие как использование выделенных линий связи или Frame Relay.

ПРИМЕЧАНИЕ Механизм IPSec, до получения сертификата на СКЗИ, может использоваться исключительно как средство построения логических каналов, без предоставления криптографической защиты.

1.3.1. Архитектура IPSec

IPSec представляет собой набор протоколов, разработанных для обеспечения защиты на сетевом уровне (уровень 3), с использованием методов шифрования и аутентификации. С точки зрения сетевого оборудования, зашифрованные пакеты маршрутизируются точно так же, как и обычные IP-пакеты. При использовании межфилиального режима VPN, поддержка IPSec требуется только на оконечных устройствах.

Существует три основных компонента архитектуры IPSec. Которыми являются:

- Протокол заголовка аутентификации (AH).
- Протокол ESP (Encapsulating Security Payload).
- Протокол IKE (Internet Key Exchange), обычно ISAKMP/Oakley.

Протокол ESP позволяет зашифровать поле данных пакета, протокол AH используется для аутентификации трафика, протокол IKE обеспечивает защищенный метод обмена криптографическими ключами, а также согласование используемых методов аутентификации и шифрования. Набор параметров IPSec, характеризующий подключение называется политикой безопасности (security policy). Политика безопасности определяет то, каким образом обе оконечных точки будут использовать сервисы безопасности (шифрование, хеширование и группы Диффи-Хеллмана). Узлы IPSec согласуют набор параметров безопасности, которые должны совпадать на обеих сторонах. После чего они устанавливают защищенное соединение (SA, security association). Защищенное соединение IPSec SA описывает логическое соединение в одном направлении. Для пакетов, которые необходимо передавать через подключение в двух направлениях, требуется два защищенных соединения: входящее и исходящее.

1.3.2. Фазы IPSec: фаза 1 и фаза 2

Установка подключения IPSec происходит в два этапа, называемые фазами IKE:

- В первой фазе IKE две оконечные точки аутентифицируют друг друга и согласовывают ключевой материал. В результате устанавливается защищенный туннель, используемый во второй фазе для согласования защищенных соединений ESP.
- Во второй фазе IKE две оконечные точки используют защищенный туннель, созданный в первой фазе, для согласования защищенных соединений ESP (ESP SA). ESP SA используются для шифрования пользовательских данных, передающихся между двумя оконечными точками.

В первой фазе IKE устанавливается защищенное соединение ISAKMP (обычно называемое, IKE SA). Протокол IKE используется для динамического согласования и аутентификации ключевого материала, а также других параметров безопасности, которые требуются для обеспечения защищенного взаимодействия. IKE использует набор из четырех протоколов (включая ISAKMP и Oakley) для динамического управления ключами в контексте IPSec.

В том случае если согласование в первой фазе IKE проходит успешно, после этого устанавливается ISAKMP SA. ISAKMP SA обычно содержит сведения "победившего предложения", к которым относятся алгоритм шифрования и ключевой материал, утвержденные в результате согласования. После чего создается безопасный канал управления ("control channel"), через который передаются ключи и другая информация, требуемая при согласовании во время второй фазы. ISAKMP SA шифрует только согласования защищенного соединения ESP во время фазы 2, а также любые сообщения IKE между двумя оконечными точками. Защищенное соединение ISAKMP SA существует в течение заранее определенного времени жизни. Время жизни настраивается на каждом из узлов VPN, а не согласуется и не передается между узлами. Указанное время жизни может быть различным на разных узлах. Когда указанное время жизни истекает, согласуется новое защищенное соединение ISAKMP SA.

Согласования второй фазы IKE также осуществляются при помощи протокола IKE. С использованием шифрования, обеспечиваемого защищенным соединением, для согласования SA второй фазы используется политика безопасности. Политика безопасности содержит сведения о взаимодействующих устройствах и подсетях, а также информацию протокола ESP для обеспечения сервисов безопасности, таких как шифрование и хеширование. Если во время второй фазы IKE процесс согласования завершится успешно, между двумя оконечными точками будет установлена пара защищенных соединений ESP SA (обычно называемых IPSec SA) — одно входящее и одно исходящее, которые будут представлять собой защищенный туннель VPN между двумя оконечными точками. С этого момента через защищенный туннель можно обмениваться пользовательскими данными.

Между двумя узлами IPSec VPN может быть установлен только один канал управления для обмена ключевым материалом во время фазы 2. Это означает, что между любыми двумя узлами будет существовать только одно защищенное соединение ISAKMP SA на каждом узле.

Между двумя узлами VPN может быть определено любое количество политик безопасности. Например, можно определить политику безопасности для создания туннеля между двумя компьютерами. Также можно определить и другую политику безопасности для создания туннеля между компьютером и подсетью, или между двумя подсетями. Так как между двумя узлами могут существовать множественные туннели, это означает, что в любой момент времени между двумя узлами могут быть активны несколько защищенных соединений IPSec SA.

1.3.3. Ключевой обмен IKE

Для того чтобы создать ISAKMP SA, два устройства должны согласовать все следующие пункты:

- Алгоритм шифрования.
- Битовую стойкость ключа шифрования (группа Диффи-Хеллмана).
- Метод аутентификации.
- Алгоритм хеширования.
- Аутентификационный материал (предварительный ключ).

Все эти сведения содержатся в предложении первой фазы IKE. На шлюзе VPN могут быть настроены несколько предложений первой фазы. Следует отметить, что время жизни SA не согласуется, а настраивается на каждом из узлов.

Во время ключевого обмена IKE, одно устройство (инициатор) отправляет первый пакет. Первый пакет содержит все предложения первой фазы, настроенные на этом узле VPN. Этот набор предложений сообщает другому шлюзу какие политики безопасности и типы аутентификации он поддерживает. Второе устройство (отвечающая сторона) изучает набор предложений и возвращает политику, обеспечивающую наилучшую защиту из предложенных, которая поддерживается обеими сторонами. Если этот процесс завершается успешно, оба устройства согласуют параметры и устанавливается защищенное соединение ISAKMP SA.

После того как ISAKMP SA было однажды установлено, эти два устройства могут использовать его для шифрования трафика второй фазы, во время которого оконечные точки пытаются согласовать IPSec SA, соответствующие принятой политике безопасности. И только после того как будут установлены защищенные соединения IPSec SA, может передаваться трафик IPSec.

Различные устройства инициируют согласование IKE по-разному. Многие устройства VPN создают туннели только по запросу. Такое устройство просматривает сетевой трафик на предмет соответствия настроенным политикам безопасности. После того как устройство получает трафик, соответствующий требуемой политике безопасности, устройство попытается установить защищенное соединение IPSec SA, которое будет использовано для расшифровки полученного трафика.

Устройства другого типа, к которым относится и Numa Edge, инициируют согласования второй фазы как только будут установлены корректные настройки политики. Если обе оконечные точки функционируют таким образом, может возникнуть состояние гонки, при котором будут созданы дублирующие друг друга защищенные соединения IPSec SA.

1.3.4. Алгоритмы шифрования

Шифрование позволяет защитить данные при их передаче по незащищенным каналам. Numa Edge поддерживает российский стандарт симметричного шифрования ГОСТ 28147-89 (**gost**).

Numa Edge поддерживает следующие алгоритмы шифрования:

- blowfish;
- cast128;
- aes;
- camellia;
- gost.

1.3.5. Алгоритмы хеширования

Хеш-функция — это функция, принимающая на вход строку битов произвольной длины и выдающая результат фиксированной длины, который называется дайджестом (digest) сообщения или хеш-значением. Хеш-функции могут использоваться для аутентификации сообщений. Numa Edge поддерживает следующие алгоритмы хеширования:

- md5;
- sha1;
- sha256;
- sha384;
- sha512;
- gosthash.

1.3.6. Предварительные ключи

По умолчанию установлен режим аутентификации с использованием предварительных ключей (PSK). В качестве предварительного ключа используется строка, заранее согласованная обеими сторонами для аутентификации сеанса. Данная строка используется для создания хеш-значения, для того чтобы оконечные точки могли аутентифицировать друг друга. Следует отметить, что предварительный ключ, несмотря на то, что это обычная строка, не является паролем в общепринятом смысле. Он фактически хешируется для формирования "отпечатка", гарантирующего подлинность каждой из сторон. Это означает, что длинные сложные строки позволяют обеспечить лучшую защиту, чем короткие строки. Следует выбирать сложные предварительные ключи и избегать коротких, которые проще скомпрометировать атакующему.

Предварительные ключи не передаются во время согласования IKE. На обеих сторонах должен быть настроен один и тот же ключ. Предварительные ключи являются типичным примером использования симметричной криптографии: когда на обеих сторонах используется

один и тот же ключ. При использовании симметричных алгоритмов шифрования две взаимодействующие стороны должны заранее обменяться ключами, используя при этом безопасные каналы связи. Асимметричные криптографические алгоритмы требуют больше вычислительных ресурсов, чем симметричные, и при том же уровне защиты им нужны более длинные ключи. Поэтому их редко используют для шифрования больших объемов данных. Чаще они применяются в протоколе защищенного обмена ключом, чтобы отправитель и получатель безопасно установили общий симметричный ключ. Асимметричные алгоритмы вместе с криптографическими хеш-функциями образуют основу цифровой подписи, которая позволяет аутентифицировать отправителя и проверить целостность сообщения.

Предварительные ключи и цифровые подписи наиболее распространенные методы аутентификации IKE. Предварительные ключи предоставляют простой и эффективный способ быстрой настройки аутентификации с небольшими накладными расходами. Однако, у этого метода есть свои недостатки.

- В том случае если предварительный ключ станет известен злоумышленнику, он будет иметь доступ к вашей сети до тех пор, пока этот ключ будет использоваться.
- Предварительные ключи настраиваются вручную, и они должны регулярно заменяться.

ПРИМЕЧАНИЕ Следует использовать предварительные ключи только в малых сетях с низким уровнем опасности.

1.3.7. Аутентификация на основе асимметричных криптографических алгоритмов

Асимметричная криптография, также известная как криптография с открытым ключом, использует класс алгоритмов, в котором применяется пара ключей: открытый ключ и секретный (закрытый) ключ, известный только его владельцу. В отличие от секретного ключа, который должен сохраняться в тайне, открытый ключ может быть общедоступным. Открытый и секретный ключ генерируются одновременно, и данные, зашифрованные одним ключом, могут быть расшифрованы при помощи другого ключа.

Криптография с открытым ключом используется при формировании и проверке ЭЦП, а также для решения проблемы безопасного распределения ключей. Одно из применений ЭЦП — аутентификация субъекта. Секретный ключ применяется для подписания данных, а открытый ключ для их проверки. Единственно известный способ получить корректную подпись — использовать секретный ключ. В целях повышения производительности подписывается не все сообщение, а его дайджест (хеш-значение). Таким образом, ЭЦП сообщения — это дайджест сообщения, зашифрованный секретным ключом, он пересылается вместе с сообщением и удостоверяет целостность сообщения и подлинность его отправителя.

Для выработки ЭЦП необходимо сгенерировать открытый и секретный ключи. Затем секретный ключ и сообщение используются как входная информация для функции генерации цифровой подписи. После того как другой пользователь получает сообщение, он использует само сообщение, связанную с ним цифровую подпись и открытый ключ для верификации (проверки) подписи. Верификация ЭЦП сообщения заключается в вычислении значения дайджеста полученного сообщения, и его сравнения со значением дайджеста в подписи, расшифрованной открытым ключом отправителя. Если значения, вычисленное получателем и сохраненного в подписи, совпадают, то считается что подпись верна, а сообщение было отправлено именно заявленным отправителем.

Особенно важным моментом при использовании схемы ЭЦП является связывание открытого ключа и субъекта, которому он принадлежит. Проблема связывания открытого ключа и субъекта может решаться разными способами, один из которых использование инфраструктуры открытых ключей (PKI) и сертификатов стандарта X.509.

1.3.8. Основные компоненты PKI

Инфраструктура открытых ключей представляет собой комплексную систему, обеспечивающую все необходимые сервисы для использования технологии открытых ключей. Неотъемлемым компонентом инфраструктуры открытых ключей является удостоверяющий центр. Непосредственное использование открытых ключей требует дополнительной их защиты и идентификации для определения связи с секретным ключом. Электронный сертификат представляет собой цифровой документ, который связывает открытый ключ с его владельцем. Для заверения электронного сертификата используется электронная цифровая подпись удостоверяющего центра (УЦ). УЦ включает свое имя в каждый выпущенный им сертификат и подписывает их при помощи собственного секретного ключа. Конечные субъекты идентифицируют сертификаты по имени УЦ, и могут убедиться в их подлинности, используя его открытый ключ.

Удостоверяющий центр выполняет следующие основные функции:

- формирует собственный секретный ключ и самоподписанный сертификат;
- выпускает сертификаты сервера и клиентов;
- ведет базу данных всех изданных сертификатов и формирует список аннулированных сертификатов;
- публикует информацию о статусе сертификатов.

Инфраструктура открытых ключей позволяет генерировать пары ключей (открытый ключ/секретный ключ). Генерация ключей может осуществляться централизованно (удостоверяющим центром) или индивидуально (конечным субъектом). В том случае если генерация ключей осуществляется конечными пользователями, они должны иметь соответствующие программные или аппаратные средства для создания надежных ключей. В том случае если пользователь не предъявляет достаточных мер для защиты своих секретных ключей, инфраструктура PKI подвергается серьезному риску.

Ключевые пары должны быть сгенерированы как для сервера VPN, так и для клиентов VPN. При установлении защищенного соединения в обязательном порядке производится аутентификация сервера VPN. Это делается для того, чтобы клиент мог быть уверен, что соединение установлено именно с тем сервером, с которым планируется обмен информацией, а не с каким-либо другим компьютером, выдающим себя за сервер.

К преимуществам централизованной генерации можно отнести быстроту создания ключей, использование специализированных средств генерации высококачественных ключей, контроль соответствия алгоритмов генерации установленным стандартам, а также хранение резервных копий на случай их утери пользователями. В том случае если ключи генерируются централизованно, они должны транспортироваться пользователям только через безопасные каналы связи.

В том случае если секретный ключ пользователя потерян, похищен или скомпрометирован, или если есть вероятность наступления таких событий, действие сертификата должно быть прекращено.

Формат сертификата определен в рекомендациях Международного союза по телекоммуникациям ITU (X.509), в настоящее время основным используемым форматом является формат версии 3.

Сертификат представляет собой структурированную двоичную запись, содержащую элементы данных, сопровождаемые цифровой подписью издателя сертификата. В сертификате имеется десять основных полей: шесть обязательных и четыре опциональных. К обязательным полям относятся:

- серийный номер сертификата Certificate Serial Number;
- идентификатор алгоритма подписи Signature Algorithm Identifier;
- имя издателя Issuer Name;

- период действия Validity (Not before / After);
- открытый ключ субъекта Subject Public Key Information;
- имя субъекта сертификата Subject Name.

В данном случае под субъектом понимается сторона, контролирующая секретный ключ, соответствующий данному открытому ключу.

Поле Version задает синтаксис сертификата. Удостоверяющий центр, выпускающий сертификат, присваивает каждому сертификату серийный номер Certificate Serial Number, который должен быть уникален.

В поле Signature Algorithm Identifier указывается идентификатор алгоритма ЭЦП, который был использован для защиты сертификата. В поле Validity (Not Before/After) указываются даты начала и окончания периода действия сертификата.

Каждый раз при использовании сертификата проверяется, является ли сертификат действующим. Сертификаты, срок действия которых истек, должны аннулироваться удостоверяющим центром.

1.3.9. Группы Диффи-Хеллмана

Схема ключевого обмена Диффи-Хеллмана используется для безопасного обмена ключами через незащищенный канал связи, например, через Интернет. Алгоритм ключевого обмена Диффи-Хеллмана был впервые опубликован в 1976 году Уитфилдом Диффи и Мартином Хеллманом.

Группы Диффи-Хелмана используются для определения длины основных простых чисел, используемых в процессе обмена ключами. Криптографическая надежность любого полученного ключа частично зависит от надежности группы Диффи-Хелмана, которая в свою очередь определяет длину используемых простых чисел. В исходной спецификации IKE определены четыре группы, называемые группами Диффи-Хеллмана или группами Oakley. Позже была определена пятая группа.

Numa Edge поддерживает следующие группы Диффи-Хеллмана:

- Группа 2 (возведение в степень по модулю MODP). Для данной группы используется длина модуля 1024 бит.
- Группа 5 (возведение в степень по модулю MODP). Для данной группы используется длина модуля 1536 бит.

1.3.10. Режимы IPSec

IPSec, в общем случае, поддерживает два режима функционирования: *агрессивный режим* и *основной режим*.

1.3.10.1. Агрессивный режим

Агрессивный режим был создан для того, чтобы уменьшить задержки во время первой фазы согласования, но он является уязвимым к атакам.

1.3.10.2. Основной режим

Установка ISAKMP SA требует отправки и приема нескольких пакетов:

- Первые два сообщения определяют политику взаимодействия.
- Следующие два сообщения включают в себя обмен параметрами Диффи-Хеллмана.
- Последние два сообщения используются для аутентификации обмена Диффи-Хеллмана.

Это стандартный способ установления соединения первой фазы, который называется *основным режимом*. Этот метод позволяет обеспечить наибольшую безопасность, так как сведения аутентификации не передаются до тех пор, пока не будет согласован обмен Диффи-Хеллмана и включено шифрование. Numa Edge поддерживает основной режим.

1.3.11. Полная безопасность пересылки

При использовании PFS (perfect forward secrecy, полная безопасность пересылки), секретный ключ используется для генерации временных (сеансовых) ключей. Сеансовые ключи не зависят друг от друга и используются в течение короткого времени, затем отбрасываются. Таким образом, если ключ скомпрометирован, это не затронет ключи, используемые в дальнейшем, а данные, которые были защищены с использованием других ключей не смогут быть раскрыты.

PFS позволяет оптимизировать как эффективность, так и безопасность. Ключи ограниченного размера позволяют ускорить вычисления, но при этом они менее защищены. При использовании PFS, можно использовать ключи ограниченного размера и часто их заменять.

1.3.12. IPSec и QoS

При использовании политик QoS работающих с маркерами поля ToS пакета IP, следует учитывать, что при инкапсуляции защищаемых туннелем IPSec пакетов в пакеты ESP и AH происходит копирование поля ToS инкапсулируемого пакета во внешний пакет IP. Тем самым, для защищённого IPSec трафика возможно применение тех же политик, что и для обычного.

В случае необходимости указания для пакетов ESP/AH конкретного значения DSCP (размещающегося в ToS) следует использовать политики модификации с фильтром для протоколов ESP и AH.

1.3.13. Фиксация изменений в настройке VPN

Подключение IPSec VPN включает в себя множество компонентов, некоторые из которых зависят друг от друга. Например, настройка подключения VPN требует корректной настройки группы IKE, корректной настройки группы ESP и корректной настройки туннеля. При фиксации настройки VPN, Numa Edge осуществляет полную проверку настройки. Если какой-либо необходимый компонент отсутствует, или настроен некорректно, фиксацию настройки осуществить не удастся.

При настройке межфилиального режима IPSec VPN должны быть корректно настроены следующие компоненты:

- Интерфейс должен быть заранее настроен, ему должен быть назначен IP-адрес.
- Узел должен быть настроен.
- Группа IKE, которая была указана в настройке узла, должна быть определена.
- Туннель должен быть настроен.
- Группа ESP, которая была указана в настройке туннеля, должна быть определена.
- Локальный IP-адрес, указанный для данного узла, должен быть назначен требуемому интерфейсу.
- Группа AH, которая была указана в настройке туннеля, должна быть определена.

В дополнение к этому, следует учесть, что изменение глобальных параметров требует перезапуска IPSec, после чего перезапускаются все туннели.

Добавление, изменение или удаление туннеля приводит к перезапуску только измененного туннеля. Изменение существующей группы IKE или группы ESP приводит к перезапуску туннеля, использующего эту группу. Изменение сведений аутентификации (предварительных ключей или электронной цифровой подписи) не влечет за собой перезапуска туннеля.

2. ПРИМЕРЫ БАЗОВОЙ НАСТРОЙКИ

2.1. Настройка базового подключения в межфилиальном режиме

ПРИМЕЧАНИЕ Там, где на практике должны быть использованы общедоступные IP-адреса, в примерах использованы IP-адреса из диапазонов 192.0.2.0/24 (TEST-NET-1), 198.51.100.0/24 (TEST-NET-2) и 203.0.113.0/24 (TEST-NET-3), описаных в RFC 5737.

В этом разделе рассматриваются следующие вопросы:

- Настройка V1.
- Настройка узла V2.

В данном разделе представлены примеры настройки базового туннеля IPSec между системами Numa Edge, которые называются соответственно V1 и V2. Сначала настраивается узел V1, затем V2. После завершения настройки, узлы будут настроены, как показано на рисунке 1.

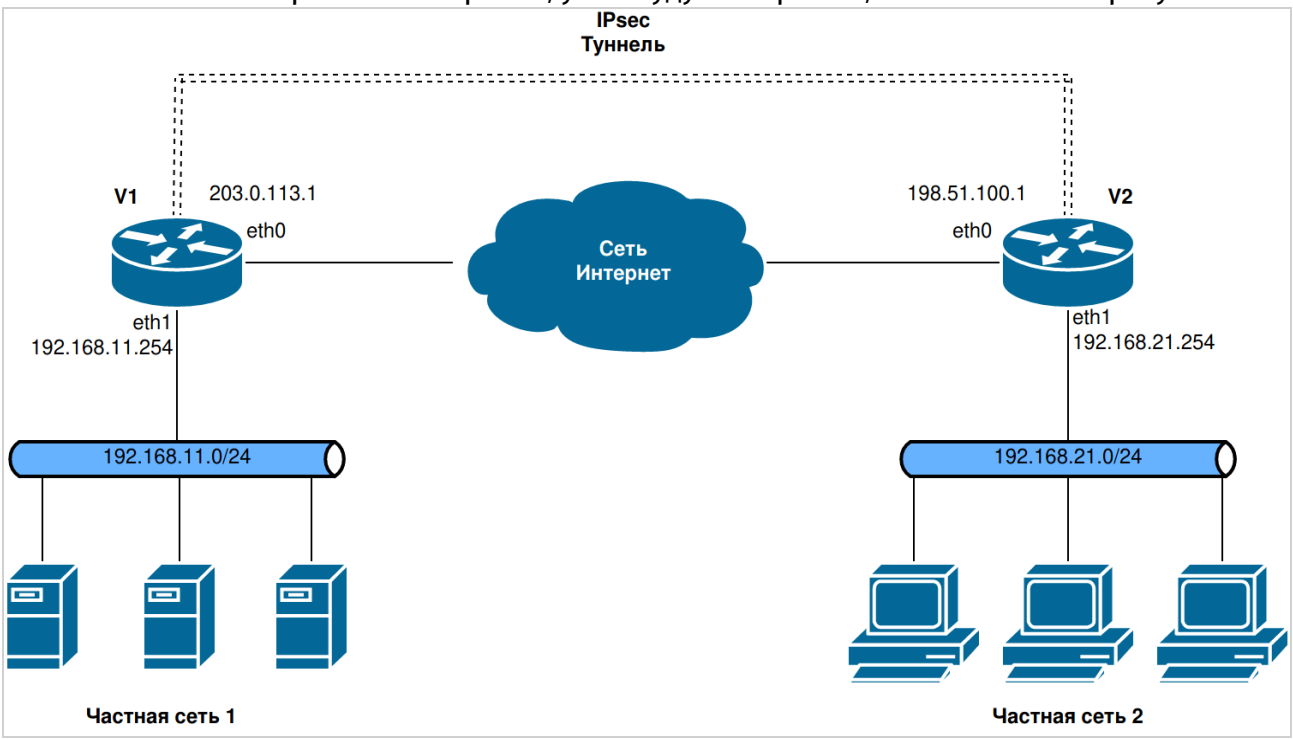


Рисунок 1 – Первичная настройка IPsec в межфилиальном режиме

Перед началом настройки:

- В этом наборе примеров, используются две системы Numa Edge, с именами узлов V1 и V2. Последний набор примеров предполагает наличие третьей системы Numa Edge с именем V3.
- Описание настройки интерфейсов ethernet выходит за рамки данного документа. Согласно схеме, интерфейсы eht0 на каждом узле будет использоваться для IPsec VPN, интерфейсы eth1 - для локальной сети.
- На интерфейсе должен быть настроен IP-адрес, который требуется использовать в качестве IP-адреса отправителя для пакетов, отправляемых шлюзу VPN. В этом примере, IP-адрес 203.0.113.1 назначен интерфейсу eth0 узла V1, и адрес 198.51.100.1 назначен интерфейсу eth0 узла V2.
- Для локальных сетей используется следующая адресация: 192.168.XY.0/24, где X - номер узла, Y - номер интерфейса этого узла.
- Для каждого узла в качестве шлюза по умолчанию используется ip-адрес X.X.X.254 где X.X.X - подсеть для интерфейса eth0.

ПРИМЕЧАНИЕ Отправка и получение сообщений ICMP о перенаправлении отключена при использовании IPsec VPN.

2.1.1. Настройка V1

В данном разделе представлены следующие примеры:

- Пример 1 – Настройка группы IKE на узле V1.
- Пример 2 – Настройка группы ESP на узле V1.
- Пример 3 – Создание подключения в межфилиальном режиме от узла V1 к узлу V2.

2.1.1.1. Настройка группы IKE на узле V1

Группа IKE позволяет предопределить набор из одного или более предложений, использующихся при согласовании первой фазы IKE, после которой сможет быть установлено защищенное соединение ISAKMP SA. Для каждого предложения в группе, необходимо определить следующее:

- Алгоритм шифрования, который будет использован для шифрования пакетов во время первой фазы IKE.
- Хеш-функция, которая будет использована для аутентификации пакетов во время первой фазы IKE.

Для группы IKE также должно быть настроено время жизни, которое представляет собой длительность защищенного соединения ISAKMP SA. Когда время жизни ISAKMP SA истекает, осуществляется новое согласование первой фазы, и для новой пары защищенных соединений ISAKMP SA устанавливается новый алгоритм шифрования, хеширования и новый ключевой материал.

Время жизни относится ко всей группе IKE в целом. То есть, если группа IKE включает в себя несколько предложений, время жизни не зависит от того, какое именно предложение было принято.

В примере 1 создается группа IKE с именем IKE-V1 на узле V1. Эта группа IKE включает в себя два предложения:

- В предложении 1 используется AES в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хеширования.
- В предложении 2 используется camellia в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хеширования.

Время жизни для этой группы IKE устанавливается равным 3600 секундам. Для создания указанной группы IKE, необходимо выполнить следующие действия на узле V1 в режиме настройки:

Пример 1 – Настройка группы IKE на узле V1

Действие	**Команда**
Создание узла конфигурации для предложения 1 группы IKE с именем IKE-V1.	`[edit]` `admin@V1# set vpn ipsec ike-group IKE-V1 proposal 1`
Установка алгоритма шифрования для предложения 1.	`[edit]` `admin@V1# set vpn ipsec ike-group IKE-V1 proposal 1 encryption aes`
Установка алгоритма хеширования для предложения 1.	`[edit]` `admin@V1# set vpn ipsec ike-group IKE-V1 proposal 1 hash sha1`
Установка алгоритма шифрования для предложения 2. В результате выполнения данной команды также будет создан узел конфигурации для предложения 2 группы	`[edit]` `admin@V1# set vpn ipsec ike-group IKE-V1 proposal 2 encryption camellia`

Действие	Команда
IKE с именем IKE-V1.	
Установка алгоритма хеширования для предложения 2.	[edit] admin@V1# set vpn ipsec ike-group IKE-V1 proposal 2 hash sha1
Установка времени жизни для группы IKE.	[edit] admin@V3# set vpn ipsec ike-group IKE-V1 lifetime 3600

Вывод настройки для группы IKE. На данном этапе настройки изменения не фиксируются.	[edit]
	admin@V1# show vpn ipsec ike-group IKE-V1
	+lifetime 3600
	+proposal 1 {
	+ encryption aes
	+ hash sha1
	+}
	+proposal 2 {
	+ encryption camellia
	+ hash sha1
	+}

2.1.1.2. Настройка группы ESP на узле V1

Протокол ESP - это протокол, который обеспечивает аутентификацию пакетов IP, а также шифрует их.

Протокол ESP согласует уникальное число для сеанса подключения, называемое индексом параметров безопасности (Security Parameter Index, SPI). Он также инициализирует последовательность номеров для пакетов, а также согласует алгоритм хеширования, который будет использоваться для аутентификации пакетов.

Numa Edge позволяет предопределить несколько настроек ESP. Каждая из них называется "группой ESP." Группа ESP включает в себя предложения второй фазы, которые содержат параметры, необходимые для того, чтобы согласовать защищенное соединение IPsec:

- Алгоритм шифрования, который будет использован для шифрования пользовательских данных, передаваемых через туннель IPsec.
- Хеш-функция, используемая для аутентификации пакетов, передаваемых через туннель IPsec.
- Время жизни защищенного соединения IPsec SA.

В примере 2 создается группа ESP с именем ESP-V1 на узле V1. Группа ESP содержит два предложения:

- В предложении 1 используется AES в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хеширования.
- В предложении 2 используется camellia в качестве алгоритма шифрования и MD5 в качестве алгоритма хеширования.

Время жизни для этой группы ESP устанавливается равным 1800 секундам. Для создания группы ESP, необходимо выполнить на узле V1 следующие действия в режиме настройки:

Пример 2 – Настройка группы ESP на узле V1

Действие	Команда
Создание узла конфигурации для предложения 1 группы ESP с именем ESP-V1	[edit] admin@V1# set vpn ipsec esp-group ESP-V1 proposal 1
Установка алгоритма шифрования для предложения 1.	[edit] admin@V1# set vpn ipsec esp-group ESP-V1 proposal 1 encryption aes

Действие	**Команда**
Установка алгоритма хеширования для предложения 1.	[edit] admin@V1# set vpn ipsec esp-group ESP-V1 proposal 1 hash hmac_sha1
Установка алгоритма шифрования для предложения 2. В результате выполнения данной команды также будет создан узел конфигурации для предложения 2 группы ESP с именем ESP-V1.	[edit] admin@V1# set vpn ipsec esp-group ESP-V1 proposal 2 encryption camellia
Установка алгоритма хеширования для предложения 2.	[edit] admin@V1# set vpn ipsec esp-group ESP-V1 proposal 2 hash hmac_md5
Установка времени жизни для группы ESP.	[edit] admin@V1# set vpn ipsec esp-group ESP-V1 lifetime 1800

Вывод настройки для группы ESP. На данном этапе настройки изменения не фиксируются.	[edit]
	admin@V1# show vpn ipsec esp-group ESP-V1
	+lifetime 1800
	+proposal 1 {
	+ encryption aes
	+ hash hmac_sha1
	+}
	+proposal 2 {
	+ encryption camellia
	+ hash hmac_md5
	+}

2.1.1.3. Создание подключения к узлу V2

При определении подключения в межфилиальном режиме, указываются сведения политики IPsec (большинство из которых уже настроены в группах IKE и ESP) и информация, необходимая для маршрутизации для двух оконечных устройств туннеля IPsec.

Локальная оконечная точка — Numa Edge. Удаленная оконечная точка - шлюз VPN, в качестве которого может быть использована другая система Numa Edge, или другой IPsec-совместимый маршрутизатор, межсетевой экран с поддержкой IPsec или концентратор VPN. Для каждой из оконечных точек туннеля, необходимо назначить IP-адрес и маску подсети для локальной и удаленной подсетей или узлов.

В целом необходимо определить следующие параметры:

- IP-адрес удаленного узла.
- Режим аутентификации, который узлы будут использовать для взаимной аутентификации. В данном наборе примеров используется аутентификация на основе предварительных ключей (PSK), то есть необходимо также указать строку, которая будет использоваться для генерации хешированного ключа.
- Группа IKE, которая будет использоваться для данного подключения.
- Группа ESP, которая будет использоваться для данного подключения.
- IP-адрес данной системы Numa Edge, который будет использоваться для данного туннеля. IP-адрес должен быть назначен заранее.
- Взаимодействующая подсеть или отдельное устройство для каждой из сторон туннеля. Для каждого узла VPN можно определить несколько туннелей, каждый из этих туннелей может использовать отдельную политику безопасности.

При использовании предварительных ключей, необходимо учитывать следующее:

По умолчанию установлен режим аутентификации с использованием предварительных ключей (PSK). В качестве предварительного ключа используется строка, заранее согласованная обеими сторонами для аутентификации сеанса. Она используется для создания хеш-значения, для того чтобы оконечные точки могли аутентифицировать друг друга.

Следует отметить, что предварительный ключ, несмотря на то, что это обычная строка, не является паролем в общепринятом смысле. Он фактически хешируется для формирования "отпечатка", гарантирующего подлинность каждой из сторон. Это означает, что длинные сложные строки позволяют обеспечить лучшую защиту, чем короткие строки. Следует выбирать сложные предварительные ключи и избегать коротких, которые проще скомпрометировать атакующему.

Предварительные ключи не передаются во время согласования IKE. На обеих сторонах должен быть настроен один и тот же ключ.

Предварительные ключи являются типичным примером использования симметрической криптографии: когда на обеих сторонах используется один и тот же ключ. Симметричные алгоритмы шифрования используют меньше вычислений, по сравнению с асимметричными алгоритмами, и, следовательно, являются более быстрыми. Однако, в симметричной криптографии, две взаимодействующие стороны должны заранее обменяться ключами. При этом должны быть использованы безопасные каналы связи.

Предварительные ключи и цифровые подписи, наиболее распространенные методы аутентификации IKE. Предварительные ключи предоставляют простой и эффективный способ быстрой настройки аутентификации с небольшими накладными расходами. Однако, у этого метода есть свои недостатки.

- В том случае если предварительный ключ станет известен злоумышленнику, он будет иметь доступ к вашей сети до тех пор, пока этот ключ будет использоваться.
- Предварительные ключи настраиваются вручную, и они должны регулярно заменяться.

Использование предварительных ключей для организации доступа удаленных пользователей аналогично выдаче им пароля от вашей сети.

ПРИМЕЧАНИЕ Следует использовать предварительные ключи только в малых сетях с низким уровнем опасности.

В примере 3 определяется подключение в межфилиальном режиме к узлу V2.

Для этого используется туннель, обеспечивающий взаимодействие между подсетью 192.168.11.0/24 на узле V1 и подсетью 192.168.21.0/24 на узле V2, с использование группы ESP с именем ESP-V1.

Используемые параметры:

- На узле V1 интерфейсу eth0 назначен IP-адрес 203.0.113.1
- На узле V2 интерфейсу eth0 назначен IP-адрес 198.51.100.1
- Используется группа IKE с именем IKE-V1
- Для аутентификации используются предварительные ключи. В качестве предварительного ключа используется строка "test_key_1".

Для настройки указанного подключения необходимо выполнить на узле V1 следующие действия в режиме настройки:

Пример 3 – Создание подключения в межфилиальном режиме от узла V1 к узлу V2

Действие	**Команда**
Создание узла конфигурации для туннеля к узлу V2.	`[edit]` `admin@V1# set vpn ipsec site-to-site peer 198.51.100.1`
Переход к другому узлу конфигурации для более удобного редактирования.	`[edit]` `admin@V1# edit vpn ipsec site-to-site peer 198.51.100.1`

Действие	**Команда**
Указание режима аутентификации.	[edit vpn ipsec site-to-site peer 198.51.100.1] admin@V1# set authentication method pre-shared-key
Ввод строки, которая будет использоваться в качестве предварительного ключа.	[edit vpn ipsec site-to-site peer 198.51.100.1] admin@V1# set authentication pre-shared-key test_key_1
Указание группы IKE.	[edit vpn ipsec site-to-site peer 198.51.100.1] admin@V1# set ike-group IKE-V1
Указание IP-адреса данной системы Numa Edge, который будет использоваться для данного туннеля.	[edit vpn ipsec site-to-site peer 198.51.100.1] admin@V1# set local-ip 203.0.113.1
Указание IP-адреса удаленного узла VPN, который будет использоваться для данного туннеля.	[edit vpn ipsec site-to-site peer 198.51.100.1] admin@V1# set remote-ip 198.51.100.1
Указание локальной подсети для данного туннеля.	[edit vpn ipsec site-to-site peer 198.51.100.1] admin@V1# set local-subnet 192.168.11.0/24
Указание удаленной подсети для данного туннеля.	[edit vpn ipsec site-to-site peer 198.51.100.1] admin@V1# set remote-subnet 192.168.21.0/24
Указание группы ESP для данного туннеля.	[edit vpn ipsec site-to-site peer 198.51.100.1] admin@V1# set esp-group ESP-V1
Возврат к вершине дерева настройки.	[edit vpn ipsec site-to-site peer 198.51.100.1] admin@V1# top
Фиксация настройки.	[edit] admin@V1# commit

Вывод настройки для подключения IPsec в межфилиальном режиме.	[edit]
	admin@V1# show vpn ipsec site-to-site peer 198.51.100.1
	authentication {
	method pre-shared-key
	pre-shared-key test_key_1
	}
	esp-group ESP-V1
	ike-group IKE-V1
	local-ip 203.0.113.1
	local-subnet 192.168.11.0/24
	nat-traversal off
	remote-ip 198.51.100.1
	remote-subnet 192.168.21.0/24

2.1.2. Настройка узла V2

В данном разделе приведены следующие примеры:

- Пример 4 – Настройка группы IKE на узле V2.
- Пример 5 – Настройка группы ESP на узле V2.
- Пример 6 – Создание подключения в межфилиальном режиме от узла V2 к узлу V1.

2.1.2.1. Настройка группы IKE на узле V2

В примере 4 создается группа IKE с именем IKE-V2 на узле V2. Группа IKE содержит два предложения:

- В предложении 1 используется AES в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хеширования.
- В предложении 2 используется camellia в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хеширования.

Время жизни для этой группы IKE устанавливается равным 3600 секундам.

Следует учесть, что указанные параметры соответствуют параметрам, установленным в группе IKE-V1 на узле V1. Необходимо убедиться при определении предложений, что указаны такие алгоритмы шифрования и хеширования, что два узла смогут согласовать хотя бы одну комбинацию параметров.

Для создания указанной группы IKE, необходимо выполнить на узле V2 следующие действия в режиме настройки:

Пример 4 – Настройка группы IKE на узле V2

Действие	**Команда**
Создание узла конфигурации для предложения 1 группы IKE с именем IKE-V2.	`[edit]` `admin@V2# set vpn ipsec ike-group IKE-V2 proposal 1`
Установка алгоритма шифрования для предложения 1.	`[edit]` `admin@V2# set vpn ipsec ike-group IKE-V2 proposal 1 encryption aes`
Установка алгоритма хеширования для предложения 1.	`[edit]` `admin@V2# set vpn ipsec ike-group IKE-V2 proposal 1 hash sha1`
Установка алгоритма шифрования для предложения 2. В результате выполнения данной команды также будет создан узел конфигурации для предложения 2 группы IKE с именем IKE-V2.	`[edit]` `admin@V2# set vpn ipsec ike-group IKE-V2 proposal 2 encryption camellia`
Установка алгоритма хеширования для предложения 2.	`[edit]` `admin@V2# set vpn ipsec ike-group IKE-V2 proposal 2 hash sha1`
Установка времени жизни для группы IKE.	`[edit]` `admin@V3# set vpn ipsec ike-group IKE-V2 lifetime 3600`

Вывод настройки для группы IKE. На данном этапе настройки изменения не фиксируются.	`[edit]`
	`admin@V2# show vpn ipsec ike-group IKE-V2`
	`+lifetime 3600`
	`+proposal 1 {`
	`+    encryption aes`
	`+    hash sha1`
	`+}`
	`+proposal 2 {`
	`+    encryption camellia`
	`+    hash sha1`
	`+}`

2.1.2.2. Настройка группы ESP на узле V2

В примере 5 создается группа ESP с именем ESP-V2 на узле V2. Группа ESP содержит два предложения:

- В предложении 1 используется AES в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хеширования.
- В предложении 2 используется camellia в качестве алгоритма шифрования и MD5 в качестве алгоритма хеширования.
- Время жизни для этой группы ESP устанавливается равным 1800 секундам. Для создания указанной группы ESP необходимо выполнить следующие действия на узле V2 в режиме настройки:

Пример 5 – Настройка группы ESP на узле V2

Действие	**Команда**
Создание узла конфигурации для предложения 1 группы ESP с именем ESP-V2.	`[edit]` `admin@V2# set vpn ipsec esp-group ESP-V2 proposal 1`
Установка алгоритма шифрования для предложения 1.	`[edit]` `admin@V2# set vpn ipsec esp-group ESP-V2 proposal 1 encryption aes`
Установка алгоритма хеширования для предложения 1.	`[edit]` `admin@V2# set vpn ipsec esp-group ESP-V2 proposal 1 hash hmac_sha1`
Установка алгоритма шифрования для предложения 2. В результате выполнения данной команды также будет создан узел конфигурации для предложения 2 группы ESP с именем ESP-V2.	`[edit]` `admin@V2# set vpn ipsec esp-group ESP-V2 proposal 2 encryption camellia`
Установка алгоритма хеширования для предложения 2.	`[edit]` `admin@V2# set vpn ipsec esp-group ESP-V2 proposal 2 hash hmac_md5`
Установка времени жизни для группы ESP.	`[edit]` `admin@V1# set vpn ipsec esp-group ESP-V2 lifetime 1800`

Вывод настройки для группы ESP. На данном этапе настройки изменения не фиксируются.	`[edit]`
	`admin@V2# show vpn ipsec esp-group ESP-V2`
	`+lifetime 1800`
	`+proposal 1 {`
	`+    encryption aes`
	`+    hash hmac_sha1`
	`+}`
	`+proposal 2 {`
	`+    encryption camellia`
	`+    hash hmac_md5`
	`+}`

2.1.2.3. Создание подключения к узлу V1

В примере 6 определяется подключение в межфилиальном режиме к узлу V1. В этом примере:

- Для этого используется туннель, обеспечивающий взаимодействие между подсетью 192.168.21.0/24 на узле V2 и подсетью 192.168.11.0/24 на узле V1, с использованием группы ESP с именем ESP-V2.
- На узле V2 интерфейсу eth0 назначен IP-адрес 198.51.100.1.
- На узле V1 интерфейсу eth0 назначен IP-адрес 203.0.113.1.
- Используется группа IKE с именем IKE-V2.

- Для аутентификации используются предварительные ключи. В качестве предварительного ключа используется строка "test_key_1".

Для настройки этого подключения необходимо выполнить следующие действия на узле V2 в режиме настройки:

Пример 6 – Создание подключения в межфилиальном режиме от узла V2 к узлу V1

Действие	**Команда**
Создание узла конфигурации для туннеля к узлу V1.	`[edit]` `admin@V2# set vpn ipsec site-to-site peer 203.0.113.1`
Переход к другому узлу конфигурации для удобства редактирования.	`[edit]` `admin@V2# edit vpn ipsec site-to-site peer 203.0.113.1`
Указание режима аутентификации.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V2# set authentication method pre-shared-key`
Ввод строки, которая будет использоваться в качестве предварительного ключа.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V2# set authentication pre-shared-key test_key_1`
Указание группы IKE.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V2# set ike-group IKE-V2`
Указание IP-адреса данной системы Numa Edge, который будет использоваться для данного подключения.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V2# set local-ip 198.51.100.1`
Указание локальной подсети для данного туннеля.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V2# set local-subnet 192.168.21.0/24`
Указание IP-адреса удаленного узла VPN, который будет использоваться для данного подключения.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V2# set remote-ip 203.0.113.1`
Указание удаленной подсети для данного туннеля.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V2# set remote-subnet 192.168.11.0/24`
Указание группы ESP для данного туннеля.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V2# set esp-group ESP-V2`
Возврат к вершине дерева настройки.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V2# top`
Фиксация настройки.	`[edit]` `admin@V2# commit`

Вывод настройки для подключения IPsec в межфилиальном режиме.	`[edit]`
	`admin@V2# show vpn ipsec site-to-site peer 203.0.113.1`
	`authentication {`
	`  method pre-shared-key`
	`  pre-shared-key test_key_1`
	`}`
	`esp-group ESP-V2`

Действие	Команда
	ike-group IKE-V2 local-ip 198.51.100.1 local-subnet 192.168.21.0/24 nat-traversal off remote-ip 203.0.113.1 remote-subnet 192.168.11.0/24

2.2. Аутентификация на основе схемы ЭЦП на базе RSA

В этом разделе рассматриваются следующие вопросы:

- Генерация ключевой пары RSA на узле V1.
- Экспорт открытого ключа узла V1 на узел V2.
- Генерация ключевой пары RSA на узле V2.
- Экспорт открытого ключа узла V2 на узел V1.
- Изменение настроек подключения к узлу V2 на узле V1.
- Изменение настроек подключения к узлу V1 на узле V2.

В этом наборе примеров изменяются параметры подключения VPN, настроенного в предыдущем наборе примеров. Для подключения, настроенного в предыдущем наборе примеров, использовалась аутентификация на основе предварительных ключей. В данном наборе примеров параметры подключения изменяются для использования аутентификации на базе криптосистемы RSA.

2.2.1. Генерация ключевой пары RSA на узле V1

В данном примере приведена генерация ключевой пары узла V1, которая будет использована для аутентификации на базе криптосистемы RSA. Ключевая пара состоит из открытого ключа и закрытого ключа. Открытый ключ должен быть доставлен узлу V2; закрытый ключ должен храниться в секрете.

Для генерации ключевой пары RSA необходимо выполнить следующие шаги на узле V1 в эксплуатационном режиме.

Пример 7 – Создание ключевой пары RSA на узле V1

Действие	Команда
Генерация ключевой пары. После выполнения команды в системное хранилище ключей IPSec добавляется ключевая пара RSA.	admin@V1$ vpn rsa-key generate v1-key Сгенерирован новый RSA ключ v1-key admin@V1$

2.2.2. Экспорт открытого ключа узла V1 на узел V2

Для осуществления проверки подлинности узлу V2 должен быть известен открытый ключ узла V1. Таким образом, после генерации ключевой пары RSA на устройстве V1, необходимо передать открытый ключ на устройство V2. Данное действие осуществляется с помощью команды vpn rsa-key export v1-key to <file>, где в качестве file – указывается расположение выходного файла, который будет передан через протокол SSH на устройство V2.

Далее, на устройстве V1 необходимо произвести импорт полученного файла в свое системное хранилище ключей.

В примере 8 приведена команда экспорта ключа узла V1 на узел V2. Имя «v1-key» используется в качестве идентификатора ключа.

Пример 8 – Создание ключевой пары RSA на узле V1

Действие	Команда
Экспорт открытого ключа с узла V1 на узел V2. Экспорт производится в домашний	admin@V1:~$ vpn rsa-key export v1-key to scp://admin@198.51.100.1/home/admin/

Действие	Команда
каталог пользователя admin на устройстве V2. Экспорт осуществляется через протокол SSH.	Производится экспорт RSA ключа в scp://admin@198.51.100.1/home/admin/v1-key Numa Edge 1.0 Password: v1-key 379 105.4KB/s 00:00 admin@V1:~$

2.2.3. Генерация ключевой пары RSA на узле V2

Аналогичным образом производится генерация ключевой пары узла V2, которая будет использована для аутентификации на базе криптосистемы RSA. Ключевая пара состоит из открытого ключа и закрытого ключа. Открытый ключ должен быть доставлен узлу V2; закрытый ключ должен храниться в секрете.

Для генерации ключевой пары RSA необходимо выполнить следующие шаги на узле V2 в эксплуатационном режиме.

Пример 9 – Генерация ключевой пары RSA для узла V2

Действие	Команда
Генерация ключевой пары. После выполнения команды в системное хранилище ключей IPSec добавляется ключевая пара RSA.	admin@V2$ vpn rsa-key generate v2-key Сгенерирован новый RSA ключ v2-key admin@V2$

2.2.4. Экспорт открытого ключа узла V2 на узел V1

Для осуществления проверки подлинности узлу V1 должен быть известен открытый ключ узла V2. Таким образом, после генерации ключевой пары RSA на устройстве V2, необходимо передать открытый ключ на устройство V1. Данное действие осуществляется с помощью команды vpn rsa-key export v2-key to <file>, где в качестве file – указывается расположение выходного файла, который будет передан через протокол SSH на устройство V1.

Далее, на устройстве V1 необходимо произвести импорт полученного файла в свое системное хранилище ключей.

В примере 10 приведена команда экспорта ключа узла V2 на узел V1. Имя "v2-key" используется в качестве идентификатора ключа.

Первоначально необходимо скопировать открытый ключ узла V2 в буфер обмена. Если на узле V1 включен эксплуатационный режим, следует перейти в режим настройки и выполнить следующие действия:

Пример 10 – Экспорт открытого ключа узла V2 на узел V1

Действие	Команда
Экспорт открытого ключа с узла V2 на узел V1. Экспорт производится в домашний каталог пользователя admin на устройстве V1. Экспорт осуществляется через протокол SSH.	admin@V2:~$ vpn rsa-key export v2-key to scp://admin@203.0.113.1/home/admin/ Производится экспорт RSA ключа в scp://admin@203.0.113.1/home/admin/v2-key Numa Edge 1.0 Password: v2-key 100% 379 105.4KB/s 00:00 admin@V2:~$

2.2.5. Изменение настроек подключения к узлу V2 на узле V1

В примере 11 изменяются параметры подключения от узла V1 к узлу V2, таким образом, чтобы использовалась аутентификация на базе RSA. В этом примере:

- В системное хранилище импортируется ранее полученный ключ узла V2.

- Установленный режим аутентификации с использованием предварительных ключей заменяется на аутентификацию на базе RSA.
- Открытый ключ узла V2 указывается в качестве удаленного ключа под именем, созданным на предыдущем шаге (Экспорт открытого ключа узла V2 на узел V1).
- Также указывается локальный ключ устройства V1, который был сгенерирован ранее.

Для изменения настройки аутентификации на использование криптосистемы RSA необходимо выполнить следующие шаги:

Пример 11 – Настройка узла V1 на использование аутентификации на базе криптосистемы RSA

Действие	**Команда**
Импорт в системное хранилище ранее экспортированного открытого ключа от узла V2.	`admin@V1:~$ vpn rsa-key import v2-key from /home/admin/v2-key` `Импортируется RSA ключ v2-key: ok`
Переход в конфигурационный режим.	`admin@V1:~$ configure`
Изменение режима аутентификации. При этом оставшийся в конфигурации pre-shared-key использоваться не будет.	`[edit]` `admin@V1# set vpn ipsec site-to-site peer 198.51.100.1 authentication method plain-rsa`
Указание идентификатора открытого ключа узла V2.	`[edit]` `admin@V1# set vpn ipsec site-to-site peer 198.51.100.1 authentication peer-key v2-key`
Указание идентификатора локального закрытого ключа.	`[edit]` `admin@V1# set vpn ipsec site-to-site peer 198.51.100.1 authentication key v1-key`
Фиксация настройки.	`[edit]` `admin@V1# commit`

Вывод измененной настройки.	`[edit]`
	`admin@V1# show vpn ipsec site-to-site peer 198.51.100.1`
	`  authentication {`
	`  key v1-key`
	`  method plain-rsa`
	`  peer-key v2-key`
	`  pre-shared-key test_key_1`
	
	`  }`
	`  esp-group ESP-V1`
	`  ike-group IKE-V1`
	`  local-ip 203.0.113.1`
	`  local-subnet 192.168.11.0/24`
	`  nat-traversal off`
	`  remote-ip 198.51.100.1`
	`  remote-subnet 192.168.21.0/24`

2.2.6. Изменение настроек подключения к узлу V1 на узле V2

В примере 12 изменяются параметры подключения от узла V2 к узлу V1, таким образом, чтобы использовалась аутентификация на базе RSA. В этом примере:

- В системное хранилище импортируется ранее полученный ключ узла V1.
- Установленный режим аутентификации с использованием предварительных ключей заменяется на аутентификацию на базе RSA.

- Открытый ключ узла V1 указывается в качестве удаленного ключа под именем, созданным на предыдущем шаге (Экспорт открытого ключа узла V2 на узел V1).
- Также указывается локальный ключ устройства V2, который был сгенерирован ранее.

Для изменения настройки аутентификации на использование криптосистемы RSA необходимо выполнить следующие шаги:

Пример 12 – Настройка узла V1 на использование аутентификации на базе криптосистемы RSA

Действие	**Команда**
Импорт в системное хранилище ранее экспортированного открытого ключа от узла V1.	`admin@V2:~$ vpn rsa-key import v1-key from /home/admin/v1-key` `Импортируется RSA ключ v1-key: ok`
Переход в конфигурационный режим.	`admin@V2:~$ configure`
Изменение режима аутентификации. При этом оставшийся в конфигурации pre-shared-key использоваться не будет.	`[edit]` `admin@V2# set vpn ipsec site-to-site peer 203.0.113.1 authentication method plain-rsa`
Указание идентификатора открытого ключа узла V1.	`[edit]` `admin@V2# set vpn ipsec site-to-site peer 203.0.113.1 authentication peer-key v1-key`
Указание идентификатора локального закрытого ключа.	`[edit]` `admin@V2# set vpn ipsec site-to-site peer 203.0.113.1 authentication key v2-key`
Фиксация настройки.	`[edit]` `admin@V2# commit`

Отображение измененной настройки для подключения в межфилиальном режиме.	`[edit]`
	`admin@V2# show vpn ipsec site-to-site peer 203.0.113.1`
	`authentication {`
	`key v2-key`
	`method plain-rsa`
	`peer-key v1-key`
	`pre-shared-key test_key_1`
	`}`
	`esp-group ESP-V2`
	`ike-group IKE-V2`
	`local-ip 198.51.100.1`
	`local-subnet 192.168.21.0/24`
	`nat-traversal off`
	`remote-ip 203.0.113.1`
	`remote-subnet 192.168.11.0/24`

2.3. Аутентификация на базе PKI

В этом разделе рассматриваются следующие вопросы:

- Создание удостоверяющего центра.
- Генерация сертификата узла V1.
- Генерация сертификата узла V2.
- Экспорт сертификата узла V2.
- Импорт сертификата узла V2.
- Изменение настроек подключения к узлу V2 на узле V1.
- Изменение настроек подключения к узлу V1 на узле V2.

В этом наборе примеров изменяются параметры подключения VPN, настроенного в наборе примеров, приведенном в разделе «Настройка базового подключения в межфилиальном режиме». Для подключения, настроенного в предыдущем наборе примеров, использовалась аутентификация на основе предварительных ключей. В данном наборе примеров параметры подключения изменяются для использования аутентификации на основе PKI X.509.

2.3.1. Создание удостоверяющего центра

В данном примере будет приведено создание удостоверяющего центра, который будет использован для управления сертификатами узлов VPN при использовании режима аутентификации на базе инфраструктуры открытых ключей стандарта X.509.

В данном примере удостоверяющий центр создается на узле V1.

На базе созданного удостоверяющего центра будет осуществляться централизованное создание и управление ключевыми парами и сертификатами узлов V1 и V2.

Для создания нового удостоверяющего центра необходимо выполнить следующие шаги на узле V1 в режиме настройки.

Пример 13 – Создание удостоверяющего центра на узле V1

Действие	**Команда**
Создание удостоверяющего центра.	`[edit]` `admin@V1# set pki ca MainCA`
Указание общего имени (common name) удостоверяющего центра.	`[edit]` `admin@V1# set pki ca MainCA cn "Main Certification Authority"`
Указание города, в качестве одного из атрибутов идентификатора УЦ.	`[edit]` `admin@V1# set pki ca MainCA city SPb`
Указание страны, в качестве одного из атрибутов идентификатора УЦ.	`[edit]` `admin@V1# set pki ca MainCA country RU`
Указание периода действия сертификата удостоверяющего центра.	`[edit]` `admin@V1# set pki ca MainCA expiration 1095`
Фиксация настройки.	`[edit]` `admin@V1# commit`

Вывод настройки.	`[edit]`
	`admin@V1# show pki ca MainCA`
	`  city SPb`
	`  cn "Main Certification Authority"`
	`  country RU`
	`  expires-on "Sat Apr 29 17:00:04 2023"`
	`  key-size 256`
	`  key-type gost2012`

2.3.2. Генерация сертификата узла V1

В данном примере будет приведено создание сертификата узла V1, который будет использован при аутентификации узлов VPN на базе инфраструктуры открытых ключей.

Для создания сертификата узла V1 необходимо выполнить следующие шаги на узле V1 в режиме настройки.

Пример 14 – Создание сертификата узла V1

Действие	**Команда**
Создание сертификата для узла V1.	`[edit]` `admin@V1# set pki ca MainCA certificate V1-cert`

Действие	**Команда**
Указание общего имени (common name), которое будет указано в сертификате узла V1.	[edit] admin@V1# set pki ca MainCA certificate V1-cert cn "V1 VPN Peer certificate"
Фиксация настройки.	[edit] admin@V1# commit
Вывод настройки созданного сертификата.	[edit] admin@V1# show pki ca MainCA certificate V1-cert cn "V1 VPN Peer certificate" expires-on "Thu Apr 29 17:01:46 2021 key-size 256 key-type gost2012

2.3.3. Генерация сертификата узла V2

В данном примере будет приведено создание сертификата узла V2, который будет использован при аутентификации узлов VPN на базе инфраструктуры открытых ключей.

Для создания сертификата узла V2 необходимо выполнить следующие шаги на узле V1 в режиме настройки.

Пример 15 – Создание сертификата узла V2

Действие	**Команда**
Создание сертификата для узла V2.	[edit] admin@V1# set pki ca MainCA certificate V2-cert
Указание общего имени (common name), которое будет указано в сертификате узла V2.	[edit] admin@V1# set pki ca MainCA certificate V2-cert cn "V2 VPN Peer certificate"
Фиксация настройки.	[edit] admin@V1# commit

Вывод настройки.	[edit]
	admin@V1# show pki ca MainCA certificate
	V1-cert {
	cn "V1 VPN Peer certificate"
	expires-on "Thu Apr 29 17:01:46 2021"
	key-size 256
	key-type gost2012
	}
	V2-cert {
	cn "V2 VPN Peer certificate"
	expires-on "Thu Apr 29 17:05:44 2021"
	key-size 256
	key-type gost2012
	}

2.3.4. Экспорт сертификата узла V2

В данном примере приведен экспорт сертификата узла V2 на флэш-накопитель. При выполнении команды **pki export certificate** <*имя*> к устройству должен быть подключен флэш-накопитель. Монтирование и размонтирование флэш-накопителя осуществляется автоматически. Экспортируемые файлы будут помещены в корневую директорию флэш-накопителя. К экспортируемым файлам относятся: сертификат удостоверяющего центра, сертификат клиента, подписанный указанным удостоверяющим центром, секретный ключ клиента и файл, содержащий список аннулированных сертификатов.

ПРИМЕЧАНИЕ При использовании команды **pki export certificate** <имя> экспортируется секретный ключ, связанный с открытым ключом, указанным в сертификате. Секретный ключ должен храниться в тайне, и не должен передаваться третьим лицам.

Для экспортирования сертификата узла V2 на флэш-накопитель необходимо выполнить следующие шаги на узле V1 в эксплуатационном режиме, к устройству должен быть заранее подключен флэш-накопитель.

Пример 16 – Экспортирование сертификата узла V2

Действие	Команда
Экспортирование сертификата узла V2, секретного ключа узла V2, сертификата удостоверяющего центра.	`admin@V1:~$ pki export certificate V2-cert`

После осуществления экспорта в корневой директории флэш-накопителя будут содержаться следующие файлы:

- cacert-MainCA.pem: сертификат удостоверяющего центра;
- cert-MainCA-V2-cert.pem: сертификат узла V2;
- crl-MainCA.pem: список отозванных сертификатов;
- pkey-MainCA-V2-cert.pem: секретный ключ узла V2.

2.3.5. Импорт сертификата узла V2

В данном примере приведен импорт сертификата узла V2 с флэш-накопителя. При выполнении команды **pki import** к устройству должен быть подключен флэш-накопитель, в корне которого должны размещаться следующие файлы:

- сертификат удостоверяющего центра;
- сертификат узла V2;
- список отозванных сертификатов;
- секретный ключ узла V2.

Монтирование и размонтирование флэш-накопителя осуществляется автоматически. В результате выполнения указанной команды в систему на узле V2 будут добавлены сертификат удостоверяющего центра, сертификат узла V2, подписанный указанным удостоверяющим центром, секретный ключ, а также файл, содержащий список аннулированных сертификатов.

Для импорта сертификата узла V2 необходимо выполнить следующие шаги на узле V2 в эксплуатационном режиме, к устройству должен быть заранее подключен флэш-накопитель.

Пример 17 – Импорт сертификата узла V2

Действие	**Команда**

Импорт сертификата узла V2, секретного ключа узла V2, сертификата удостоверяющего центра, списка отозванных сертификатов.	`admin@V2:~$ pki import`
	`Импортируется CA: Main Certification Authority`
	`Импортируется CRL для Main_Certification_Authority`
	`Импортируется сертификат: V2 VPN Peer certificate`

2.3.6. Изменение настроек подключения к узлу V2 на узле V1

В примере 18 изменяются параметры подключения от узла V1 к узлу V2, таким образом, чтобы использовалась аутентификация на основе использования инфраструктуры открытых ключей. В этом примере:

- Установленный режим аутентификации с использованием предварительных ключей заменяется на аутентификацию на основе инфраструктуры открытых ключей на базе X.509.

• В настройке указывается сертификат узла V1, созданный на предыдущем шаге (см. Генерация сертификата узла V1).

Для изменения настройки аутентификации на использование инфраструктуры открытых ключей на базе X.509 необходимо выполнить следующие шаги в режиме настройки на узле V1:

Пример 18 – Настройка узла V1 на использование аутентификации на базе инфраструктуры открытых ключей

Действие	**Команда**
Изменение режима аутентификации.	[edit] admin@V1# set vpn ipsec site-to-site peer 198.51.100.1 authentication method x509
Указание используемого имени сертификата узла V1.	[edit] admin@V1# set vpn ipsec site-to-site peer 198.51.100.1 authentication x509-cert V1-cert
Фиксация настройки.	[edit] admin@V1# commit

Отображение измененной настройки подключения в межфилиальном режиме.	[edit]
	admin@V1# show vpn ipsec site-to-site peer
	198.51.100.1 {
	authentication {
	method x509
	pre-shared-key test_key_1
	x509-cert V1-cert
	}
	esp-group ESP-V1
	ike-group IKE-V1
	local-ip 203.0.113.1
	local-subnet 192.168.11.0/24
	remote-ip 198.51.100.1
	remote-subnet 192.168.21.0/24
	}

2.3.7. Изменение настроек подключения к узлу V1 на узле V2

В примере 19 изменяются параметры подключения от узла V2 к узлу V1 таким образом, чтобы для аутентификации использовалась инфраструктура открытых ключей на базе X.509.

В этом примере:

• Ранее установленный режим аутентификации с использованием предварительных ключей заменяется на аутентификацию на основе инфраструктуры открытых ключей.

• В настройке указывается сертификат узла V2, импортированный на предыдущем шаге (см. раздел «Импорт сертификата узла V2»).

Для изменения настройки аутентификации на использование инфраструктуры открытых ключей необходимо выполнить следующие шаги в режиме настройки на узле V2:

Пример 19 – Настройка узла V2 для аутентификации с использованием X.509

Действие	**Команда**
Изменение режима аутентификации.	[edit] admin@V2# set vpn ipsec site-to-site peer 203.0.113.1 authentication method x509
Указание используемого имени сертификата	[edit] admin@V2# set vpn ipsec site-to-site

Действие	**Команда**
узла V1. При импорте сертификата, в качестве его названия используется CN.	`peer 203.0.113.1 authentication x509-cert V2_VPN_Peer_certificate`
Фиксация настройки.	`[edit]` `admin@V2# commit`

Отображение измененной настройки подключения в межфилиальном режиме.	`[edit]`
	`admin@V2# show vpn ipsec site-to-site peer`
	`  203.0.113.1 {`
	`  authentication {`
	`  method x509`
	`  pre-shared-key test_key_1`
	`  x509-cert V2_VPN_Peer_certificate`
	`  }`
	`  esp-group ESP-V2`
	`  ike-group IKE-V2`
	`  local-ip 198.51.100.1`
	`  local-subnet 192.168.21.0/24`
	`  nat-traversal off`
	`  remote-ip 203.0.113.1`
	`  remote-subnet 192.168.11.0/24`
	`  }`

2.4. Настройка туннелей IPSec между тремя шлюзами

В этом разделе рассматриваются следующие вопросы:

- Настройка узла V1.
- Настройка узла V2.
- Настройка узла V3.

В данном разделе представлен пример настройки подключения в межфилиальном режиме между тремя шлюзами: V1, V2, и V3. После завершения настройки все узлы будут настроены, как показано на рисунке ниже

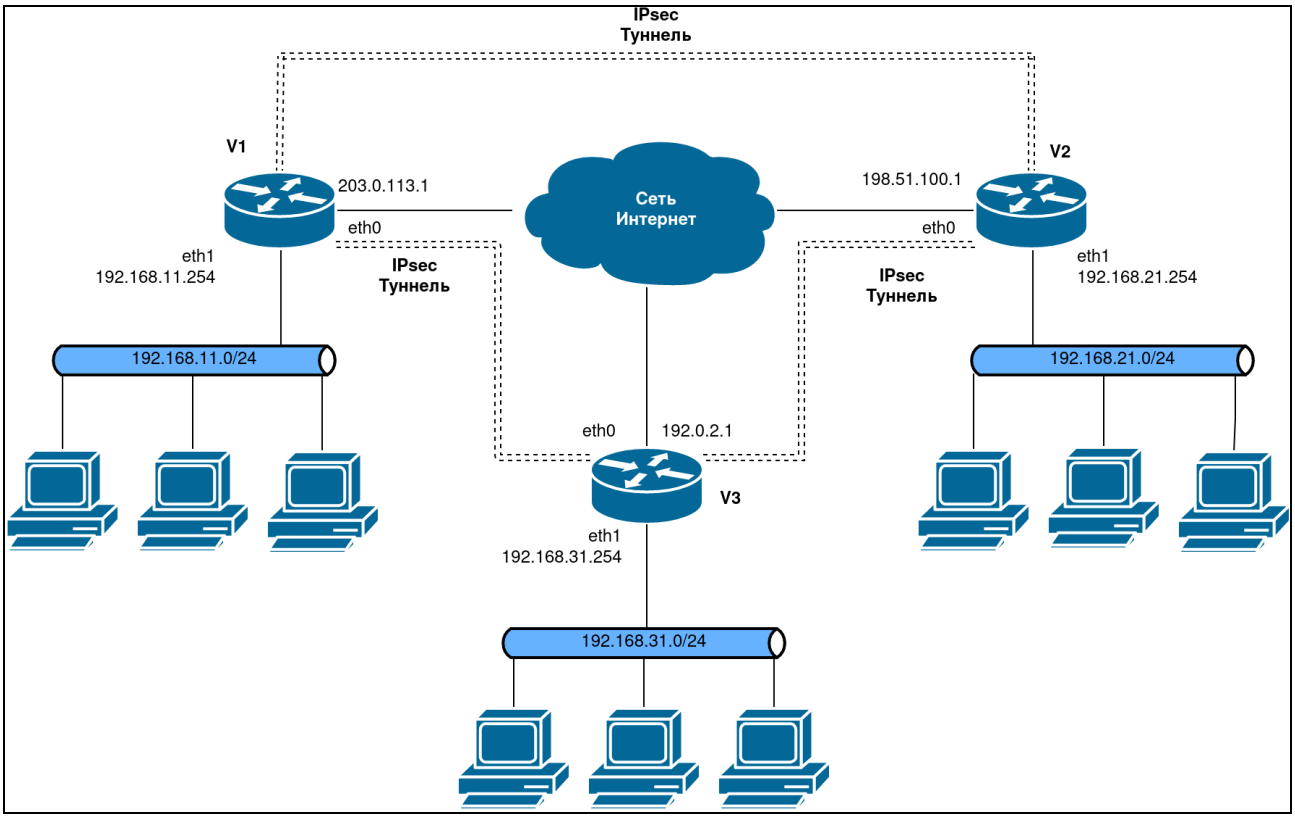


Рисунок 2 – Настройка туннелей IPsec между тремя шлюзами

2.4.1. Настройка узла V1

В этом разделе рассматриваются следующие вопросы:

- Создание подключения к узлу V3.

В данном примере предполагается, что на узле V1 уже настроено базовое подключение к узлу V2, как показано в примере «Настройка базового подключения в межфилиальном режиме».

Дополнительная настройка узла V1 для данного примера заключается в создании нового подключения в межфилиальном режиме к узлу V3.

В данном разделе представлены следующие пример 21 создания подключения от узла V1 к узлу V3 в межфилиальном режиме.

2.4.1.1. Создание подключения к узлу V3

В примере 20 определяется подключение в межфилиальном режиме от узла V1 к узлу V3.

Туннель обеспечит подключение между подсетью 192.168.11.0/24 на узле V1 и подсетью 192.168.31.0/24 на узле V3, с использованием группы ESP с именем ESP-V1.

- На узле V1 интерфейсу eth0 назначен IP-адрес 203.0.113.1.
- На узле V3 интерфейсу eth0 назначен IP-адрес 192.0.2.1.
- Используется группа IKE с именем IKE-V1
- Используется группа ESP с именем ESP-V1.
- В качестве предварительного ключа используется строка "test_key_2".

Для настройки указанного туннеля необходимо выполнить следующие шаги на узле V1 в режиме настройки:

Пример 20 – Создание туннеля от узла V1 к узлу V3 в межфилиальном режиме

Действие	**Команда**
Создание узла конфигурации для туннеля к узлу V3	`[edit]` `admin@V1#set vpn ipsec site-to-site peer 192.0.2.1`
Переход к другому узлу конфигурации для более	`[edit]`

Действие	**Команда**
удобного редактирования	`admin@V1# edit vpn ipsec site-to-site peer 192.0.2.1`
Указание режима аутентификации.	`[edit vpn ipsec site-to-site peer 192.0.2.1` `admin@V1# set authentication method pre-shared-key`
Ввод строки, которая будет использоваться в качестве предварительного ключа.	`[edit vpn ipsec site-to-site peer 192.0.2.1]` `admin@V1# set authentication pre-shared-key test_key_2`
Указание группы IKE.	`[edit vpn ipsec site-to-site peer 192.0.2.1]` `admin@V1# set ike-group IKE-V1`
Указание IP-адреса данной системы Numa Edge, который будет использоваться для этого подключения.	`[edit vpn ipsec site-to-site peer 192.0.2.1]` `admin@V1# set local-ip 203.0.113.1`
Указание локальной подсети для этого туннеля.	`[edit vpn ipsec site-to-site peer 192.0.2.1]` `admin@V1# set local-subnet 192.168.11.0/24`
Указание IP-адреса удаленного шлюза, который будет использоваться для этого подключения.	`[edit vpn ipsec site-to-site peer 192.0.2.1]` `admin@V1# set remote-ip 192.0.2.1`
Указание удаленной подсети для туннеля.	`[edit vpn ipsec site-to-site peer 192.0.2.1]` `admin@V1# set remote-subnet 192.168.31.0/24`
Указание группы ESP для туннеля.	`[edit vpn ipsec site-to-site peer 192.0.2.1]` `admin@V1# set esp-group ESP-V1`
Возврат к вершине дерева настройки.	`[edit vpn ipsec site-to-site peer 192.0.2.1]` `admin@V1# top`
Фиксация настройки.	`[edit]` `admin@V1# commit`

Вывод настройки для подключения IPSec в межфилиальном режиме.	`[edit]`
	`admin@V1# show vpn ipsec site-to-site peer 192.0.2.1`
	` authentication {`
	`  method pre-shared-key`
	`  pre-shared-key test_key_2`
	` }`
	` esp-group ESP-V1`
	` ike-group IKE-V1`
	` local-ip 203.0.113.1`
	` local-subnet 192.168.11.0/24`
	` nat-traversal off`
	` remote-ip 192.0.2.1`
	` remote-subnet 192.168.31.0/24`

2.4.2. Настройка узла V2

В этом разделе рассматриваются следующие вопросы:

- Создание подключения к узлу V3.

В данном примере предполагается, что на узле V2 уже настроено базовое подключение к узлу V1, как показано в примере «Настройка базового подключения в межфилиальном режиме».

Дополнительная настройка узла V2 для данного примера заключается в создании нового подключения в межфилиальном режиме к узлу V3.

2.4.2.1. Создание подключения к узлу V3

В примере 21 определяется подключение в межфилиальном режиме от узла V2 к узлу V3.

Туннель обеспечит подключение между подсетью 192.168.21.0/24 на узле V2 и подсетью 192.168.31.0/24 на узле V3, с использованием группы ESP с именем ESP-V1.

- На узле V2 интерфейсу eth1 назначен IP-адрес 198.51.100.1.
- На узле V3 интерфейсу eth1 назначен IP-адрес 192.0.2.1.
- Используется группа IKE с именем IKE-V1
- Используется группа ESP с именем ESP-V1.
- В качестве предварительного ключа используется строка "test_key_2".

Для настройки указанного туннеля необходимо выполнить следующие шаги на узле V1 в режиме настройки:

Пример 21 – Создание подключения в межфилиальном режиме от узла V2 к узлу V3

Действие	**Команда**
Создание узла конфигурации для туннеля к узлу V3	`[edit]` `admin@V2#set vpn ipsec site-to-site peer 192.0.2.1`
Переход к этому узлу конфигурации для более удобного редактирования	`[edit]` `admin@V2# edit vpn ipsec site-to-site peer 192.0.2.1`
Указание режима аутентификации.	`[edit vpn ipsec site-to-site peer 192.0.2.1]` `admin@V2# set authentication method pre-shared-key`
Ввод строки, которая будет использоваться в качестве предварительного ключа.	`[edit vpn ipsec site-to-site peer 192.0.2.1]` `admin@V2# set authentication pre-shared-key test_key_2`
Указание группы IKE.	`[edit vpn ipsec site-to-site peer 192.0.2.1]` `admin@V2# set ike-group IKE-V2`
Указание IP-адреса данной системы Numa Edge, который будет использоваться для этого подключения.	`[edit vpn ipsec site-to-site peer 192.0.2.1]` `admin@V2# set local-ip 198.51.100.1`
Указание локальной подсети для этого туннеля.	`[edit vpn ipsec site-to-site peer 192.0.2.1]` `admin@V2# set local-subnet 192.168.21.0/24`
Указание IP-адреса удаленного шлюза VPN.	`[edit vpn ipsec site-to-site peer 192.0.2.1]` `admin@V2# set remote-ip 192.0.2.1`
Указание удаленной подсети для туннеля.	`[edit vpn ipsec site-to-site peer 192.0.2.1]` `admin@V2# set remote-subnet 192.168.31.0/24`
Указание группы ESP для туннеля.	`[edit vpn ipsec site-to-site peer`

Действие	Команда
	192.0.2.1] admin@V2# set esp-group ESP-V2
Возврат к вершине дерева настройки.	[edit vpn ipsec site-to-site peer 192.0.2.1] admin@V2# top
Фиксация настройки.	[edit] admin@V2# commit

Вывод настройки для подключения IPsec в межфилиальном режиме.	[edit]
	admin@V2# show vpn ipsec site-to-site peer 192.0.2.1
	authentication {
	method pre-shared-key
	pre-shared-key test_key_2
	}
	esp-group ESP-V2
	ike-group IKE-V2
	local-ip 198.51.100.1
	local-subnet 192.168.21.0/24
	remote-ip 192.0.2.1
	remote-subnet 192.168.31.0/24

2.4.3. Настройка узла V3

В этом разделе рассматриваются следующие вопросы:

- Настройка группы IKE на узле V3.
- Настройка группы ESP на узле V3.
- Создание подключения к узлу V1.
- Создание подключения к узлу V2.

В этом разделе представлены следующие примеры:

- Пример 22 – Настройка группы IKE на узле V3.
- Пример 23 – Настройка группы ESP на узле V3.
- Пример 24 – Создание туннеля в межфилиальном режиме от узла V3 к узлу V1.
- Пример 25 – Создание подключения в межфилиальном режиме от узла V3 к узлу V2.

2.4.3.1. Настройка группы IKE на узле V3

В примере 22 приведено создание группы IKE с именем IKE-1S на узле V3. Данная группа IKE содержит два предложения:

- В предложении 1 используется AES в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хеширования.
- В предложении 2 используется camellia в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хеширования.

Время жизни для этой группы IKE устанавливается равным 3600 секундам.

Следует учесть, что указанные параметры соответствуют параметрам, установленным в группе IKE-V1 на узле V1 и в группе IKE-V2 на узле V2. Необходимо убедиться, при определении предложений, что указанные алгоритмы шифрования и хеширования таковы, что два узла смогут согласовать хотя бы одну комбинацию параметров.

Для создания указанной группы IKE необходимо выполнить следующие шаги на узле V3 в режиме настройки:

Пример 22 – Настройка группы IKE на узле V3

Действие	**Команда**
Создание узла конфигурации для предложения 1 группы IKE с именем IKE-1S.	`[edit]` `admin@V3# set vpn ipsec ike-group IKE-1S proposal 1`
Установка алгоритма шифрования для предложения 1.	`[edit]` `admin@V3# set vpn ipsec ike-group IKE-1S proposal 1 encryption aes`
Установка алгоритма хеширования для предложения 1.	`[edit]` `admin@V3# set vpn ipsec ike-group IKE-1S proposal 1 hash sha1`
Установка алгоритма шифрования для предложения 2. В результате выполнения данной команды также будет создан узел конфигурации для предложения 2 группы IKE с именем IKE-1S.	`[edit]` `admin@V3# set vpn ipsec ike-group IKE-1S proposal 2 encryption camellia`
Установка алгоритма хеширования для предложения 2.	`[edit]` `admin@V3# set vpn ipsec ike-group IKE-1S proposal 2 hash sha1`
Установка времени жизни для группы IKE.	`[edit]` `admin@V3# set vpn ipsec ike-group IKE-1S lifetime 3600`

Вывод настройки для группы IKE. На данном этапе настройки изменения не фиксируются.	`admin@V3# show vpn ipsec ike-group`
	`+IKE-1S {`
	`+  lifetime 3600`
	`+  proposal 1 {`
	`+  encryption aes`
	`+  hash sha1`
	`+  }`
	`+  proposal 2 {`
	`+  encryption camellia`
	`+  hash sha1`
	`+  }`
	`+}`
	`[edit]`

2.4.3.2. Настройка группы ESP на узле V3

В примере 23 приведено создание группы ESP с именем ESP-1S на узле V3. Данная группа ESP содержит два предложения:

- В предложении 1 используется AES в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хеширования.
- В предложении 2 используется camellia в качестве алгоритма шифрования и MD5 в качестве алгоритма хеширования. Время жизни для предложений этой группы ESP устанавливается равным 1800 секундам. Для создания указанной группы ESP необходимо выполнить следующие шаги на узле V3 в режиме настройки:

Пример 23 – Настройка группы ESP на узле V3

Действие	**Команда**
Создание узла конфигурации для предложения 1 группы ESP с именем ESP-1S.	`[edit]` `admin@V3# set vpn ipsec esp-group ESP-1S proposal 1`
Установка алгоритма шифрования для	`[edit]`

Действие	Команда
предложения 1.	admin@V3# set vpn ipsec esp-group ESP-1S proposal 1 encryption aes
Установка алгоритма хеширования для предложения 1.	[edit] admin@V3# set vpn ipsec esp-group ESP-1S proposal 1 hash hmac_sha1
Установка алгоритма шифрования для предложения 2. В результате выполнения данной команды также будет создан узел конфигурации для предложения 2 группы ESP с именем ESP-1S.	[edit] admin@V3# set vpn ipsec esp-group ESP-1S proposal 2 encryption camellia
Установка алгоритма хеширования для предложения 2.	[edit] admin@V3# set vpn ipsec esp-group ESP-1S proposal 2 hash hmac_md5
Установка времени жизни для группы ESP.	[edit] admin@V3# set vpn ipsec esp-group ESP-1S lifetime 1800

Вывод настройки для группы ESP. На данном этапе настройки изменения не фиксируются.	[edit]
	admin@V3# show vpn ipsec esp-group ESP-1S
	+ lifetime 1800
	+ proposal 1 {
	+ encryption aes
	+ hash hmac_sha1
	}
	+ proposal 2 {
	+ encryption camellia
	+ hash hmac_md5
	}

2.4.3.3. Создание подключения к узлу V1

В примере 24 приведено определение подключения в межфилиальном режиме к узлу V1.

Туннель обеспечивает взаимодействие между подсетью 192.168.31.0/24 на узле V3 и подсетью 192.168.11.0/24 на узле V1 с использованием группы ESP с именем ESP-1S.

На узле V3 интерфейсу eth0 назначен IP-адрес 192.0.2.1.

На узле V1 интерфейсу eth0 назначен IP-адрес 203.0.113.1.

Используется группа IKE с именем IKE-1S.

В качестве предварительного ключа используется строка "test_key_2".

Для настройки этого туннеля необходимо выполнить следующие действия на узле V3 в режиме настройки:

Пример 24 – Создание туннеля в межфилиальном режиме от узла V3 к узлу V1

Действие	Команда
Создание узла конфигурации для туннеля к узлу V1.	[edit] admin@V3# set vpn ipsec site-to-site peer 203.0.113.1
Переход к этому узлу конфигурации для более удобного редактирования.	[edit] admin@V3# edit vpn ipsec site-to-site peer 203.0.113.1
Указание режима аутентификации.	[edit vpn ipsec site-to-site peer 203.0.113.1] admin@V3#set authentication method pre-shared-key

Действие	**Команда**
Ввод строки, которая будет использоваться в качестве предварительного ключа.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V3# set authentication pre-shared-key test_key_2`
Указание группы IKE.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V3# set ike-group IKE-1S`
Указание локального IP-адреса данной системы Numa Edge, который будет использоваться для этого подключения.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V3# set local-ip 192.0.2.1`
Указание локальной подсети для этого туннеля.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V3# set local-subnet 192.168.31.0/24`
Указание IP-адреса удаленного шлюза VPN.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V3# set remote-ip 203.0.113.1`
Указание удаленной подсети для туннеля 1.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V3# set remote-subnet 192.168.11.0/24`
Указание группы ESP для туннеля.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V3# set esp-group ESP-1S`
Возврат к вершине дерева настройки.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V3# top`
Фиксация настройки.	`[edit]` `admin@V3# commit`

Вывод настройки для подключения IPsec в межфилиальном режиме.	`[edit]`
	`admin@V3# show vpn ipsec site-to-site peer 203.0.113.1`
	` authentication {`
	`  method pre-shared-key`
	`  pre-shared-key test_key_2`
	` }`
	` esp-group ESP-1S`
	` ike-group IKE-1S`
	` local-ip 192.0.2.1`
	` local-subnet 192.168.31.0/24`
	` remote-ip 203.0.113.1`
	` remote-subnet 192.168.11.0/24`

2.4.3.4. Создание подключения к узлу V2

В примере 25 приведено определение подключения в межфилиальном режиме к узлу V2.

Туннель обеспечивает взаимодействие между подсетью 192.168.31.0/24 на узле V3 и подсетью 192.168.21.0/24 на узле V2 с использованием группы ESP с именем ESP-1S.

На узле V3 интерфейсу eth0 назначен IP-адрес 192.0.2.1.

На узле V2 интерфейсу eth0 назначен IP-адрес 198.51.100.1.

Используется группа IKE с именем IKE-1S.

В качестве предварительного ключа используется строка "test_key_2".

Для настройки этого подключения необходимо выполнить следующие действия на узле V3 в режиме настройки:

Пример 25 – Создание подключения в межфилиальном режиме от узла V3 к узлу V2

Действие	**Команда**
Создание узла конфигурации для туннеля к узлу V2	`[edit]` `admin@V3# set vpn ipsec site-to-site peer 198.51.100.1`
Переход к другому узлу конфигурации для более удобного редактирования.	`[edit]` `admin@V3# edit vpn ipsec site-to-site peer 198.51.100.1`
Установка режима аутентификации.	`[edit vpn ipsec site-to-site peer 198.51.100.1]` `admin@V3#set authentication method pre-shared-key`
Ввод строки, которая будет использоваться в качестве предварительного ключа.	`[edit vpn ipsec site-to-site peer 198.51.100.1]` `admin@V3# set authentication pre-shared-key test_key_2`
Указание группы IKE.	`[edit vpn ipsec site-to-site peer 198.51.100.1]` `admin@V3# set ike-group IKE-1S`
Указание IP-адреса данной системы Numa Edge, который будет использоваться для этого подключения.	`[edit vpn ipsec site-to-site peer 198.51.100.1]` `admin@V3# set local-ip 192.0.2.1`
Указание локальной подсети для этого туннеля.	`[edit vpn ipsec site-to-site peer 198.51.100.1]` `admin@V3# set local-subnet 192.168.31.0/24`
Указание IP-адреса шлюза VPN.	`[edit vpn ipsec site-to-site peer 198.51.100.1]` `admin@V3# set remote-ip 198.51.100.1`
Указание удаленной подсети для туннеля.	`[edit vpn ipsec site-to-site peer 198.51.100.1]` `admin@V3# set remote-subnet 192.168.21.0/24`
Указание группы ESP для туннеля.	`[edit vpn ipsec site-to-site peer 198.51.100.1]` `admin@V3# set esp-group ESP-1S`
Возврат к вершине дерева настройки.	`[edit vpn ipsec site-to-site peer 198.51.100.1]` `admin@V3# top`
Фиксация настройки.	`[edit]` `admin@V3# commit`

Вывод настройки для подключения IPsec в межфилиальном режиме.	`[edit]`
	`admin@V3# show vpn ipsec site-to-site peer 198.51.100.1`
	`authentication {`
	`method pre-shared-key`
	`pre-shared-key test_key_2`
	`}`
	`esp-group ESP-1S`
	`ike-group IKE-1S`
	`local-ip 192.0.2.1`

Действие	Команда

	`local-subnet 192.168.31.0/24`
	`remote-ip 198.51.100.1`
	`remote-subnet 192.168.21.0/24`

2.5. Создание подключения VPN с использованием NAT

В этом разделе рассматриваются следующие вопросы:

- Настройка узла V1.
- Настройка узла V2.
- Настройка узла V3.

ПРИМЕЧАНИЕ В случае необходимости настройки IPsec на том же устройстве, на котором осуществляется NAT необходимо обратиться к Руководству Администратора, раздел «Маскировка и VPN». В этом разделе рассматривается случай, когда устройство, осуществляющее NAT, находится между узлами, устанавливающими VPN соединение.

При осуществлении NAT, шлюз NAT подставляет другой IP-адрес источника (а в некоторых случаях и номер порта) вместо исходного IP-адреса и порта исходящих пакетов. Устройство NAT ожидает ответа и, после того как ответный пакет получен, осуществляет обратную замену, в результате входящий пакет доходит до нужного узла назначения. Таким образом, IP-адреса внутренней сети "скрыты" от внешних сетей.

Для обеспечения целостности данных запрещается какое-либо их изменение в процессе передачи. Это является основным препятствием, с которым можно столкнуться при реализации NAT и IPsec. Поскольку NAT изменяет заголовок IP, то это влияет на проверку целостности пакета IP в случае использования протокола AH. При любом режиме (транспортном или туннельном) протокол AH осуществляет аутентификацию всего пакета IP, включая и заголовок IP.

IPsec может быть использован в двух режимах передачи: транспортном и туннельном. При транспортном - реальный IP-заголовок (следовательно, и IP-адрес) остается нетронутым, а заголовок IPsec вставляется между заголовком IP и остальными заголовками или, соответственно, данными. При таком способе передачи обеспечивается защита только для транспортного уровня пакета IP, а, следовательно, изменение адреса отправителя и получателя не нарушит целостность пакета с точки зрения IPsec. Однако, если пакет является TCP или UDP пакетом, NAT должен рассчитывать заново контрольную сумму, которая в свою очередь защищена протоколом ESP, то есть целостность пакета с точки зрения IPsec будет нарушена.

При использовании туннельного режима изменяется весь пакет IP. Защита распространяется на заголовок IP и данные, причем вместо исходного создается новый заголовок IP с другими IP-адресами. В этом случае проблемы могут возникнуть при использовании IKE в основном режиме и аутентификации с помощью предварительных ключей. Если происходит идентификация IP-адреса партнера по заранее заданному паролю, то изменение этого IP-адреса при использовании NAT может привести к сложностям с аутентификацией. Однако если идентификация партнера IPsec происходит на основе идентификационных данных (ID) пользователя, то такая проблема не возникает.

Вышеописанную проблему позволяет решить NAT Traversal (NAT-T). Протокол IPsec NAT Traversal (NAT-T, RFCs 3947 и 3948) вкладывает IPsec пакет в пакет UDP, который может быть корректно обработан устройством, осуществляющим NAT. Протокол NAT-T функционирует поверх IPsec. Для поддержки NAT-T, межсетевой экран должен быть настроен таким образом, чтобы разрешать:

- Протокол IKE через порт UDP с номером 500.
- IPsec NAT-T через порт UDP с номером 4500.
- ESP.

ПРИМЕЧАНИЕ Протокол AH вычисляет цифровую подпись пакета перед отправкой его адресату. Протокол AH проводит процедуру аутентификации каждого пакета, обеспечивая аутентификацию заголовков IP-пакетов, несмотря на нахождение IP-заголовков за пределами создаваемого им конверта. Аутентификация AH предотвращает манипулирование полями IP-заголовка во время прохождения пакета, поэтому данный протокол нельзя применять в среде, где используется механизм трансляции сетевых адресов, так как манипулирование IP-заголовками необходимо для его работы. Поэтому протокол AH совместно с NAT-T применяться не может, так как система NAT изменяет заголовок IP, нарушая его целостность.

Некоторые шлюзы позволяют разрешить этот набор с помощью опции "Прохождение IPsec" (IPsec Pass-through). Однако, использование IPsec Pass-through несовместимо с использованием NAT-T.

ПРИМЕЧАНИЕ При включении поддержки протокола NAT-T, необходимо убедиться в том, что использование опции IPsec Pass-through на устройстве, осуществляющем NAT отключено.

В данном разделе представлен пример настройки подключения, проходящего через NAT между узлами V1, V2 и V3.

- Узлы V2 и V3 расположены за устройством, осуществляющим NAT, и по этой причине с точки зрения узла V1 они имеют динамические IP-адреса.
- Узел V1 сохраняет фиксированный IP-адрес.

После завершения настройки примеров данного раздела, узлы будут настроены, как показано на рисунке ниже.

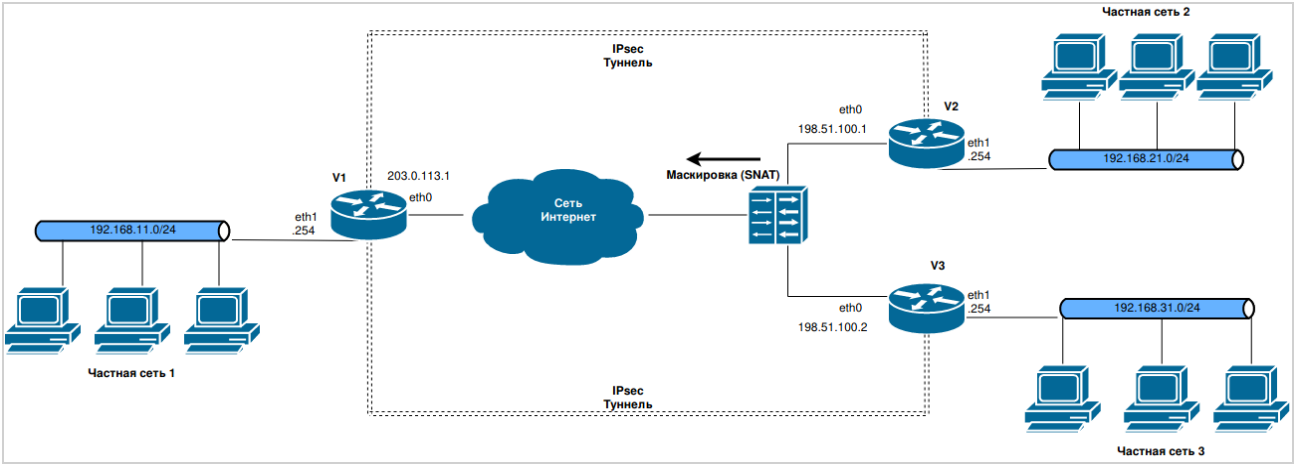


Рисунок 3 – Создание подключения VPN с использованием NAT

Перед началом настройки:

Данный пример предполагает, что основное подключение в межфилиальном режиме уже было настроено с использованием предварительных ключей для аутентификации между узлами V1, V2 см. раздел «Настройка базового подключения в межфилиальном режиме». В данном разделе представлены только необходимые изменения в настройке.

2.5.1. Настройка узла V1

Для того чтобы разрешить динамический IP-адрес узла V2, на узле V1 необходимо отредактировать существующее подключение *198.51.100.1.* Так же необходимо создать отдельное подключение к узлу V3 с названием *198.51.100.2.*

В данном разделе приведены следующие примеры:

- Пример 26 – Изменение настройки подключения от узла V2 к узлу V1
- Пример 27 – Создание подключения в межфилиальном режиме к узлу, имеющему динамический IP-адрес

2.5.1.1. Редактирование подключения к узлу V2

Для редактирования этого подключения необходимо выполнить следующие шаги на узле V1 в режиме конфигурации:

- Изменение удаленного адреса (**remote-ip**) со статического на динамический.
- Для аутентификации узлов VPN необходимо указать значение идентификаторов (узлы конфигурации **id**, **remote-id**).
- Включение NAT-Traversal.

В конфигурацию узла V1 необходимо добавить настройку аутентификации узлов:

Пример 26 – Изменение настройки подключения от узла V2 к узлу V1

Действие	**Команда**
Переход к другому узлу конфигурации для более удобного редактирования.	`[edit]` `admin@V1#edit vpn ipsec site-to-site peer 198.51.100.1`
Указание идентификатора локального узла.	`[edit vpn ipsec site-to-site peer 198.51.100.1]` `admin@V1# set authentication id V1`
Указание идентификатора удаленного узла.	`[edit vpn ipsec site-to-site peer 198.51.100.1]` `admin@V1# set authentication remote-id V2`
Указание того, что локальный узел имеет динамический адрес.	`[edit vpn ipsec site-to-site peer 198.51.100.1]` `admin@V1# set remote-ip 0.0.0.0`
Включение режима NAT Traversal.	`[edit vpn ipsec site-to-site peer 198.51.100.1]` `admin@V1#set nat-traversal on`
Возврат к вершине дерева настройки.	`[edit vpn ipsec site-to-site peer 198.51.100.1]` `admin@V1# top`
Фиксация настройки.	`[edit]` `admin@V1# commit`

Вывод настройки для подключения IPsec в межфилиальном режиме.	`[edit]`
	`admin@V1# show vpn ipsec site-to-site peer 198.51.100.1`
	`authentication`
	`{`
	`  id V1`
	`  method pre-shared-key`
	`  pre-shared-key test_key_1`
	`  remote-id V2`
	`}`
	`esp-group ESP-V1`
	`ike-group IKE-V1`
	`local-ip 203.0.113.1`
	`local-subnet 192.168.11.0/24`
	`nat-traversal on`
	`remote-ip 0.0.0.0`
	`remote-subnet 192.168.21.0/24`

Устройство, осуществляющее NAT, отслеживает фиксированный IP-адрес узла V2 и корректно маршрутизирует узлу V2 входящие пакеты, внося все необходимые изменения в исходящие пакеты.

Узел V1 сохраняет фиксированный IP-адрес, таким образом, не требуется никаких дополнительных изменений IP-адреса удаленного узла.

2.5.1.2. Создание подключения к узлу V3

В примере 27 определяется подключение в межфилиальном режиме от узла V1 к узлу V3.

Туннель обеспечит подключение между подсетью 192.168.11.0/24 на узле V1 и подсетью 192.168.31.0/24 на узле V3, с использованием группы ESP с именем ESP-V1.

- На узле V1 интерфейсу eth0 назначен IP-адрес 203.0.113.1.
- На узле V3 используется динамический удаленный адрес (узел конфигурации **remote-ip**).
- Используется группа IKE с именем IKE-V1
- Используется группа ESP с именем ESP-V1.
- В качестве предварительного ключа используется строка "test_key_2".
- Для аутентификации узлов VPN необходимо указать значение идентификаторов (узлы конфигурации **id**, **remote-id**)
- Для прохождения через NAT необходимо использовать протокол NAT-Traversal

Для настройки указанного туннеля необходимо выполнить следующие шаги на узле V1 в режиме настройки:

Пример 27 – Создание подключения в межфилиальном режиме к узлу, имеющему динамический IP-адрес

Действие	**Команда**
Создание узла конфигурации для узла V2, установка IP-адреса.	`[edit]` `admin@V1# set vpn ipsec site-to-site peer 198.51.100.2`
Переход к другому узлу конфигурации для более удобного редактирования.	`[edit]` `admin@V1# edit vpn ipsec site-to-site peer 198.51.100.2`
Установка режима аутентификации.	`[edit vpn ipsec site-to-site peer 198.51.100.2]` `admin@V1# set authentication method pre-shared-key`
Ввод строки, которая будет использоваться в качестве предварительного ключа.	`[edit vpn ipsec site-to-site peer 198.51.100.2]` `admin@V1# set authentication pre-shared-key test_key_2`
Указание группы IKE.	`[edit vpn ipsec site-to-site peer 198.51.100.2]` `admin@V1# set ike-group IKE-V1`
Указание IP-адреса данной системы Numa Edge, который будет использоваться для этого подключения.	`[edit vpn ipsec site-to-site peer 198.51.100.2]` `admin@V1# set local-ip 203.0.113.1`
Указание динамического ip-адреса для удаленного узла.	`[edit vpn ipsec site-to-site peer 198.51.100.2]` `admin@V1# set remote-ip 0.0.0.0`
Включение режима NAT Traversal.	`[edit vpn ipsec site-to-site peer 198.51.100.2]` `admin@V1#set nat-traversal on`
Указание идентификатора локального узла.	`[edit vpn ipsec site-to-site peer 198.51.100.2]` `admin@V1# set authentication id V1`
Указание идентификатора удаленного узла.	`[edit vpn ipsec site-to-site peer`

Действие	Команда
	198.51.100.2] admin@V1# set authentication remote-id V3
Создание настройки туннеля, и указание локальной подсети для данного туннеля.	[edit vpn ipsec site-to-site peer 198.51.100.2] admin@V1# set local-subnet 192.168.11.0/24
Указание удаленной подсети для данного туннеля.	[edit vpn ipsec site-to-site peer 198.51.100.2] admin@V1# set remote-subnet 192.168.31.0/24
Указание группы ESP для данного туннеля.	[edit vpn ipsec site-to-site peer 198.51.100.2] admin@V1# set esp-group ESP-V1
Возврат к вершине дерева настройки.	[edit vpn ipsec site-to-site peer 198.51.100.2] admin@V1# top
Фиксация настройки.	[edit] admin@V1# commit

Вывод настройки для подключения IPsec в межфилиальном режиме.	[edit]
	admin@V1# show vpn ipsec site-to-site peer 198.51.100.2
	authentication
	{
	id V1
	method pre-shared-key
	pre-shared-key test_key_1
	remote-id V3
	}
	esp-group ESP-V1
	ike-group IKE-V1
	local-ip 203.0.113.1
	local-subnet 192.168.11.0/24
	nat-traversal on
	remote-ip 0.0.0.0
	remote-subnet 192.168.31.0/24

2.5.2. Настройка узла V2

Для того чтобы разрешить динамический IP-адрес узла V2, на узле V1 необходимо отредактировать существующее подключение *198.51.100.1.*

В данном разделе приведен пример 28, в котором редактируется подключение к узлу V1

2.5.2.1. Редактирование подключения к узлу V1

Для редактирования этого подключения необходимо выполнить следующие шаги на узле V1 в режиме конфигурации:

- Изменение локального адреса (**local-ip**) со статического на динамический.
- Для аутентификации узлов VPN необходимо указать значение идентификаторов (узлы конфигурации **id**, **remote-id**).
- Включение NAT-Traversal

В конфигурацию узла V1 необходимо добавить настройку аутентификации узлов:

Пример 28 – Изменение настройки подключения от узла V2 к узлу V1

Действие	Команда

Действие	**Команда**
Переход к другому узлу конфигурации для более удобного редактирования.	`[edit]` `admin@V2#edit vpn ipsec site-to-site peer 203.0.113.1`
Указание идентификатора локального узла.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V2# set authentication id V2`
Указание идентификатора удаленного узла.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V2# set authentication remote-id V1`
Указание того, что локальный узел имеет динамический адрес.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V2# set local-ip 0.0.0.0`
Включение режима NAT Traversal.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V2#set nat-traversal on`
Возврат к вершине дерева настройки.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V1# top`
Фиксация настройки.	`[edit]` `admin@V1# commit`

Вывод настройки для подключения IPsec в межфилиальном режиме.	`[edit]`
	`admin@V2# show vpn ipsec site-to-site peer 203.0.113.1`
	`authentication`
	`{`
	`  id V2`
	`  method pre-shared-key`
	`  pre-shared-key test_key_1`
	`  remote-id V1`
	`}`
	`esp-group ESP-V2`
	`ike-group IKE-V2`
	`local-ip 0.0.0.0`
	`local-subnet 192.168.11.0/24`
	`nat-traversal on`
	`remote-ip 203.0.113.1`
	`remote-subnet 192.168.21.0/24`

2.5.3. Настройка узла V3

В этом разделе рассматриваются следующие вопросы:

- Настройка группы IKE на узле V3.
- Настройка группы ESP на узле V3.
- Создание подключения к узлу V1.

В этом разделе представлены следующие примеры:

- Пример 29 – Настройка группы IKE на узле V3.
- Пример 30 – Настройка группы ESP на узле V3.
- Пример 31 – Создание туннеля в межфилиальном режиме от узла V3 к узлу V1.

2.5.3.1. Настройка группы IKE на узле V3

В примере 29 приведено создание группы IKE с именем IKE-V3 на узле V3. Данная группа IKE содержит два предложения:

- В предложении 1 используется AES в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хеширования.
- В предложении 2 используется camellia в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хеширования.

Время жизни для этой группы IKE устанавливается равным 3600 секундам.

Следует учесть, что указанные параметры соответствуют параметрам, установленным в группе IKE-V1 на узле V1 и в группе IKE-V2 на узле V2. Необходимо убедиться, при определении предложений, что указанные алгоритмы шифрования и хеширования таковы, что два узла смогут согласовать хотя бы одну комбинацию параметров.

Для создания указанной группы IKE необходимо выполнить следующие шаги на узле V3 в режиме настройки:

Пример 29 – Настройка группы IKE на узле V3

Действие	**Команда**
Создание узла конфигурации для предложения 1 группы IKE с именем IKE-V3.	`[edit]` `admin@V3# set vpn ipsec ike-group IKE-V3 proposal 1`
Установка алгоритма шифрования для предложения 1.	`[edit]` `admin@V3# set vpn ipsec ike-group IKE-V3 proposal 1 encryption aes`
Установка алгоритма хеширования для предложения 1.	`[edit]` `admin@V3# set vpn ipsec ike-group IKE-V3 proposal 1 hash sha1`
Установка алгоритма шифрования для предложения 2. В результате выполнения данной команды также будет создан узел конфигурации для предложения 2 группы IKE с именем IKE-V3.	`[edit]` `admin@V3# set vpn ipsec ike-group IKE-V3 proposal 2 encryption camellia`
Установка алгоритма хеширования для предложения 2.	`[edit]` `admin@V3# set vpn ipsec ike-group IKE-V3 proposal 2 hash sha1`
Установка времени жизни для группы IKE.	`[edit]` `admin@V3# set vpn ipsec ike-group IKE-V3 lifetime 3600`

Вывод настройки для группы IKE. На данном этапе настройки изменения не фиксируются.	`admin@V3# show vpn ipsec ike-group`
	`+IKE-V3 {`
	`+ lifetime 3600`
	`+ proposal 1 {`
	`+ encryption aes`
	`+ hash sha1`
	`+ }`
	`+ proposal 2 {`
	`+ encryption camellia`
	`+ hash sha1`
	`+ }`
	`+}`
	`[edit]`

2.5.3.2. Настройка группы ESP на узле V3

В примере 30 приведено создание группы ESP с именем ESP-1S на узле V3. Данная группа ESP содержит два предложения:

- В предложении 1 используется AES в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хеширования.

- В предложении 2 используется camellia в качестве алгоритма шифрования и MD5 в качестве алгоритма хеширования. Время жизни для предложений этой группы ESP устанавливается равным 1800 секундам. Для создания указанной группы ESP необходимо выполнить следующие шаги на узле V3 в режиме настройки:

Пример 30 – Настройка группы ESP на узле V3

Действие	**Команда**
Создание узла конфигурации для предложения 1 группы ESP с именем ESP-1S.	`[edit]` `admin@V3# set vpn ipsec esp-group ESP-V3 proposal 1`
Установка алгоритма шифрования для предложения 1.	`[edit]` `admin@V3# set vpn ipsec esp-group ESP-V3 proposal 1 encryption aes`
Установка алгоритма хеширования для предложения 1.	`[edit]` `admin@V3# set vpn ipsec esp-group ESP-V3 proposal 1 hash hmac_sha1`
Установка алгоритма шифрования для предложения 2. В результате выполнения данной команды также будет создан узел конфигурации для предложения 2 группы ESP с именем ESP-V3.	`[edit]` `admin@V3# set vpn ipsec esp-group ESP-V3 proposal 2 encryption camellia`
Установка алгоритма хеширования для предложения 2.	`[edit]` `admin@V3# set vpn ipsec esp-group ESP-V3 proposal 2 hash hmac_md5`
Установка времени жизни для группы ESP.	`[edit]` `admin@V3# set vpn ipsec esp-group ESP-V3 lifetime 1800`

Вывод настройки для группы ESP. На данном этапе настройки изменения не фиксируются.	`[edit]`
	`admin@V3# show vpn ipsec esp-group ESP-V3`
	`+ lifetime 1800`
	`+ proposal 1 {`
	`+  encryption aes`
	`+  hash hmac_sha1`
	`+ }`
	`+ proposal 2 {`
	`+  encryption camellia`
	`+  hash hmac_md5`
	`+ }`

2.5.3.3. Создание подключения к узлу V1

В примере 31 приведено определение подключения в межфилиальном режиме к узлу V1.

Туннель обеспечивает взаимодействие между подсетью 192.168.31.0/24 на узле V3 и подсетью 192.168.11.0/24 на узле V1 с использованием группы ESP с именем ESP-V3.

- На узле V3 используется динамический локальный адрес (узел конфигурации **local-ip**).
- На узле V1 интерфейсу eth0 назначен IP-адрес 203.0.113.1.
- Используется группа IKE с именем IKE-V3.
- В качестве предварительного ключа используется строка "test_key_2".
- Для аутентификации узлов VPN необходимо указать значение идентификаторов (узлы конфигурации **id**, **remote-id**)
- Для прохождения через NAT необходимо использовать протокол NAT-Traversal

Для настройки этого туннеля необходимо выполнить следующие действия на узле V3 в режиме настройки:

Пример 31 – Создание туннеля в межфилиальном режиме от узла V3 к узлу V1

Действие	**Команда**
Создание узла конфигурации для туннеля к узлу V1.	[edit] admin@V3# set vpn ipsec site-to-site peer 203.0.113.1
Переход к этому узлу конфигурации для более удобного редактирования.	[edit] admin@V3# edit vpn ipsec site-to-site peer 203.0.113.1
Указание режима аутентификации.	[edit vpn ipsec site-to-site peer 203.0.113.1] admin@V3#set authentication method pre-shared-key
Ввод строки, которая будет использоваться в качестве предварительного ключа.	[edit vpn ipsec site-to-site peer 203.0.113.1] admin@V3# set authentication pre-shared-key test_key_2
Указание группы IKE.	[edit vpn ipsec site-to-site peer 203.0.113.1] admin@V3# set ike-group IKE-V3
Указание локального IP-адреса данной системы Numa Edge, который будет использоваться для этого подключения.	[edit vpn ipsec site-to-site peer 203.0.113.1] admin@V3# set local-ip 0.0.0.0
Указание локальной подсети для этого туннеля.	[edit vpn ipsec site-to-site peer 203.0.113.1] admin@V3# set local-subnet 192.168.31.0/24
Указание IP-адреса удаленного шлюза VPN.	[edit vpn ipsec site-to-site peer 203.0.113.1] admin@V3# set remote-ip 203.0.113.1
Указание удаленной подсети для туннеля 1.	[edit vpn ipsec site-to-site peer 203.0.113.1] admin@V3# set remote-subnet 192.168.11.0/24
Указание группы ESP для туннеля.	[edit vpn ipsec site-to-site peer 203.0.113.1] admin@Vremote-id V13# set esp-group ESP-V3
Указание идентификатора локального узла.	[edit vpn ipsec site-to-site peer 203.0.113.1] admin@V2# set authentication id V3
Указание идентификатора удаленного узла.	[edit vpn ipsec site-to-site peer 203.0.113.1] admin@V2# set authentication remote-id V1
Включение режима NAT Traversal.	[edit vpn ipsec site-to-site peer 203.0.113.1] admin@V2#set nat-traversal on
Возврат к вершине дерева настройки.	[edit vpn ipsec site-to-site peer 203.0.113.1] admin@V3# top
Фиксация настройки.	[edit] admin@V3# commit

Действие	**Команда**

Вывод настройки для подключения IPSec в межфилиальном режиме.	[edit]
	admin@V3# show vpn ipsec site-to-site
	peer 203.0.113.1
	authentication {
	id V3
	method pre-shared-key
	pre-shared-key test_key_2
	remote-id V1
	}
	esp-group ESP-V3
	ike-group IKE-V3
	local-ip 0.0.0.0
	local-subnet 192.168.31.0/24
	nat-traversal on
	remote-ip 203.0.113.1
	remote-subnet 192.168.11.0/24

2.6. Защита туннеля GRE с использованием IPSec

GRE, IP-in-IP, и SIT туннели не шифруются и не обеспечивают никакой защиты помимо использования паролей, которые в свою очередь передаются отрытым текстом в каждом пакете. Это означает, что GRE, IP-IP и SIT туннели, сами по себе, не обеспечивают адекватной защиты.

В то же время, туннели IPSec не могут напрямую маршрутизировать не-IP трафик или широковещательные протоколы. IPsec также имеет ряд ограничений с эксплуатационной точки зрения. Использование туннельных интерфейсов в сочетании с IPsec позволяет обеспечить безопасные, маршрутизируемые подключения между шлюзами, которые имеют некоторые преимущества по сравнению с использованием туннелей на основе IPSec:

- Поддержка стандартных эксплуатационных команд, например, **show interfaces**.
- Поддержка таких средств, как **traceroute** и SNMP.
- Динамическое переключение на другой туннель в случае отказа.
- Упрощенные политики IPsec и выявление неисправностей.

В данном наборе примеров приводится настройка IPsec в транспортном режиме между V1 и V2, внутрь которого инкапсулируется GRE туннель.

После завершения настройки узлы V1 и V2 будут настроены, как показано на рисунке ниже.

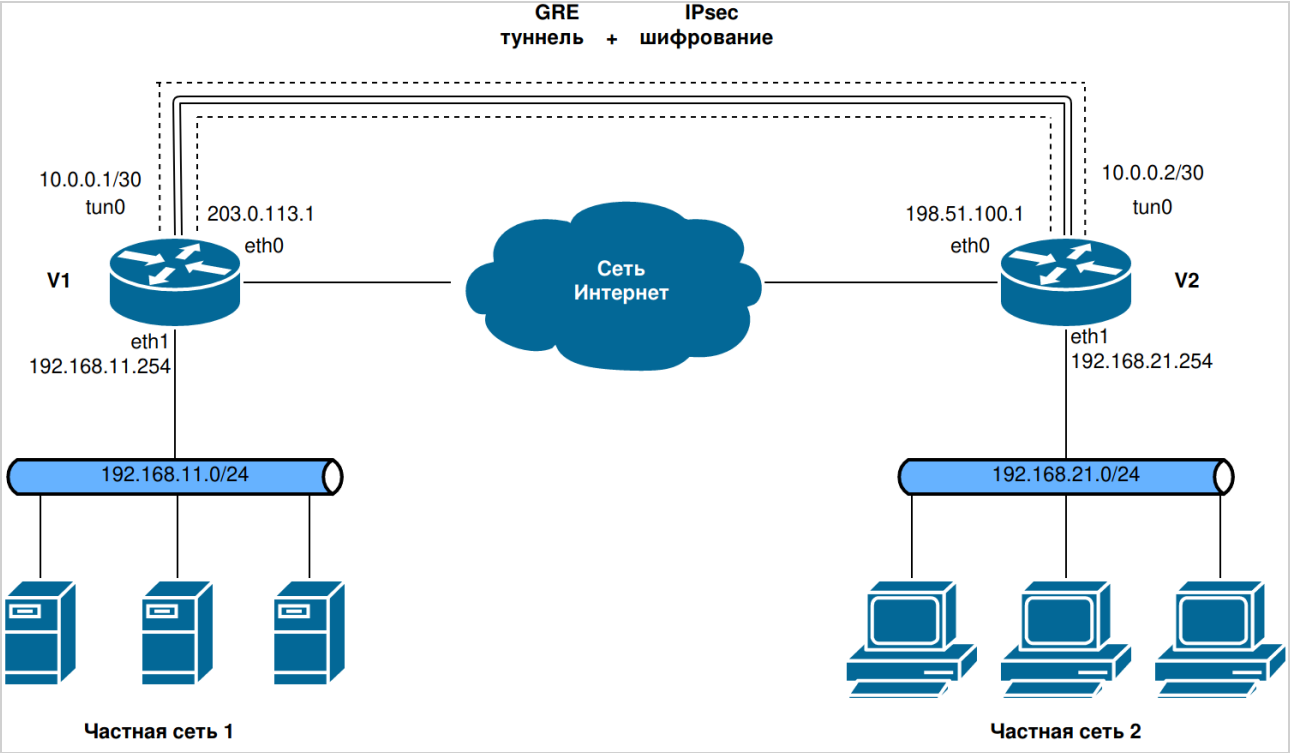


Рисунок 4 – Создание подключения в межфилиальном режиме от узла V1 к узлу V2

2.6.1. Настройка узла V1

В этом разделе представлены следующие примеры:

- Определение туннеля GRE на узле V1.
- Изменение режима работы ESP.
- Определение настроек IPsec на узле V1.
- Определение статического маршрута на узле V1.

2.6.1.1. Определение туннеля GRE на узле V1

В примере 32 определяется оконечный узел V1 туннеля GRE. В этом примере:

- Туннельному интерфейсу tun0 на маршрутизаторе V1 назначен IP-адрес 10.0.0.1/30.
- В качестве IP-адреса локального узла туннеля GRE (**local-ip**) назначен адрес интерфейса eth0 203.0.113.1.
- В качестве IP-адреса удаленного оконечного узла туннеля GRE (**remote-ip**) назначен адрес интерфейса eth0 удаленной системы 198.51.100.1.
- Указание значения MTU для GRE туннеля.

ПРИМЕЧАНИЕ Накладные расходы на каждый передаваемый пакет ESP в транспортном режиме с инкапсулированным GRE туннелем составляют 56 байт (туннельный режим добавляет еще 20 байт из-за создания нового IP заголовка). По умолчанию значение MTU для создаваемых туннелей равно 1476 байта, в то время как значение по умолчанию для ethernet интерфейсов составляет 1500 байт. Поскольку фрагментация пакетов негативно влияет на производительность VPN туннелей, хорошей практикой при использовании GRE с шифрованием IPsec указывать значение mtu равное 1400 вне зависимости от режима ESP.

Для создания туннельного интерфейса и оконечного узла V1 необходимо выполнить следующие действия в режиме настройки:

Пример 32 – Определение туннеля GRE от узла V1 к узлу V2

Действие	**Команда**
Создание туннельного интерфейса GRE, и	`[edit]`

Действие	Команда
указание связанного с ним IP-адреса.	admin@V1# set interfaces tunnel tun0 address 10.0.0.1/30
Указание локального IP-адреса туннеля GRE.	[edit] admin@V1# set interfaces tunnel tun0 local-ip 203.0.113.1
Указание удаленного IP-адреса туннеля GRE.	[edit] admin@V1# set interfaces tunnel tun0 remote-ip 198.51.100.1
Указание режима инкапсуляции для туннеля.	[edit] admin@V1# set interfaces tunnel tun0 encapsulation gre
Изменение MTU.	[edit] admin@V1# set interfaces tunnel tun0 mtu 1400
Фиксация настройки.	[edit] admin@V1# commit

Вывод настройки.	[edit]
	admin@V1# show interfaces tunnel tun0
	{
	address 10.0.0.1/30
	encapsulation gre
	local-ip 203.0.113.1
	multicast disable
	mtu 1400
	remote-ip 198.51.100.1
	ttl 255
	}

2.6.1.2. Изменение режима работы ESP

В примере 33 приведено изменение режима работы группы ESP.

В данном примере предполагается, что уже настроена группа ESP с именем ESP-1V.

Пример 33 – Изменение режима работы ESP

Действие	Команда
Изменение режима работы ESP на транспортный режим.	[edit] admin@V1#set vpn ipsec esp-group ESP-1V mode transport
Фиксация изменений	[edit] admin@V1# commit

Вывод настроек группы ESP	[edit]
	admin@V1# show vpn ipsec esp-group ESP-V1
	lifetime 1800
	mode transport
	proposal 1 {
	encryption aes
	hash hmac_sha1
	}
	proposal 2 {
	encryption camellia
	hash hmac_md5
	}

ПРИМЕЧАНИЕ Этот пример отличается от предыдущих примеров IPsec, в которых в качестве подсетей в настройке IPsec были указаны локальная и удаленная подсети, расположенные за шлюзами VPN. В данном случае будет шифроваться только трафик, который направлен от узла V1 к узлу V2, и наоборот. Основным отличием транспортного и туннельного режима работы IPsec является то, что в транспортном режиме используется оригинальный заголовок IP пакета.

2.6.1.3. Определение настроек IPsec на узле V1

В примере ниже приведено создание туннеля IPsec от узла V1 к узлу V2.

- На узле V1 интерфейсу eth0 назначен IP-адрес 203.0.113.1.
- На узле V2 интерфейсу eth0 назначен IP-адрес 198.51.100.1.
- Используется группа IKE с именем IKE-V1.
- В качестве предварительного ключа используется строка "test_key_1".
- IPsec обеспечивает шифрование между адресом 203.0.113.1 узла V1 и адресом 198.51.100.1 узла V2 и использует группу ESP с именем ESP-V2.

В данном примере предполагается, что уже настроена группа IKE с именем IKE-V1.

Для создания туннеля IPsec от узла V1 к узлу V2, необходимо выполнить следующие шаги на узле V1 в режиме настройки:

Пример 34 – Определение туннеля IPsec от узла V1 к узлу V2

Действие	**Команда**
Определение туннеля в межфилиальном режиме к узлу V2.	`[edit]` `admin@V1# set vpn ipsec site-to-site peer 198.51.100.1`
Переход к другому узлу конфигурации для более удобного редактирования.	`[edit]` `admin@V1# edit vpn ipsec site-to-site peer 198.51.100.1`
Установка режима аутентификации.	`[edit]` `admin@V1# set authentication method pre-shared-key`
Ввод строки, которая будет использоваться для аутентификации узлов.	`[edit vpn ipsec site-to-site peer 198.51.100.1]` `admin@V1# set authentication pre-shared-key test_key_1`
Указание группы IKE.	`[edit vpn ipsec site-to-site peer 198.51.100.1]` `admin@V1# set ike-group IKE-V1`
Указание IP-адреса данной системы Numa Edge, который будет использоваться для этого подключения.	`[edit vpn ipsec site-to-site peer 198.51.100.1] admin@V1# set local-ip 203.0.113.1`
Указание IP-адреса удаленного шлюза VPN.	`[edit vpn ipsec site-to-site peer 198.51.100.1]` `admin@V1# set remote-ip 198.51.100.1`
Указание группы ESP для данного туннеля.	`[edit vpn ipsec site-to-site peer 198.51.100.1]` `admin@V1# set esp-group ESP-V1`
Возврат к вершине дерева настройки.	`[edit vpn ipsec site-to-site peer 198.51.100.1]` `admin@V1# top`
Фиксация настройки.	`[edit]` `admin@V1# commit`

Действие	**Команда**

Вывод настройки.	[edit]
	admin@V1# show vpn ipsec site-to-site
	peer 198.51.100.1 authentication {
	method pre-shared-key
	pre-shared-key test_key_1
	}
	ike-group IKE-V1
	local-ip 203.0.113.1
	remote-ip 198.51.100.1
	esp-group ESP-V1

2.6.1.4. Определение статического маршрута на узле V1

В примере 35 создается статический маршрут до подсети на узле V2 через GRE туннель.

Отправка трафика, предназначенного для подсети 192.168.21.0/24, через туннельный интерфейс tun0. Для создания статического маршрута необходимо выполнить на узле V1 следующие действия в режиме настройки:

Пример 35 – Определение статического маршрута на узле V1

Действие	Команда
Создание статического маршрута.	[edit] admin@V1# set protocols static interface-route 192.168.21.0/24 next- hop-interface tun0
Фиксация настройки.	[edit] admin@V1# commit

Вывод настройки.	[edit]
	admin@V1# show protocols
	static interface-route 192.168.21.0/24
	{
	next-hop-interface tun0
	}

2.6.2. Настройка узла V2

В этом разделе представлены следующие примеры:

- Пример 36 - Определение туннеля GRE от узла V2 к узлу V1.
- Пример 37 – Изменение режима работы ESP.
- Пример 38 – Создание туннеля IPsec от узла V2 к узлу V1.
- Пример 39 – Определение статического маршрута на узле V2.

2.6.2.1. Определение туннеля GRE на узле V2

В примере 36 приведено определение оконечного узла V2 туннеля GRE. В этом примере:

- Туннельному интерфейсу tun0 на маршрутизаторе V2 назначен IP-адрес 10.0.0.2/30.
- В качестве IP-адреса локального узла туннеля (**local-ip**) назначен адрес интерфейса eth0 198.51.100.1.
- В качестве IP-адреса удаленного оконечного узла туннеля (**remote-ip**) назначен адрес интерфейса eth0 удаленной системы 203.0.113.1.
- Указание значения MTU для GRE туннеля.

Для создания туннельного интерфейса и оконечного узла V2 необходимо выполнить следующие действия в режиме настройки:

Пример 36 - Определение туннеля GRE от узла V2 к узлу V1

Действие	**Команда**
Создание туннельного интерфейса GRE, и	[edit]

Действие	Команда
указание связанного с ним IP-адреса.	admin@V2# set interfaces tunnel tun0 address 10.0.0.2/30
Указание локального IP-адреса туннеля GRE.	[edit] admin@V2# set interfaces tunnel tun0 local-ip 198.51.100.1
Указание удаленного IP-адреса туннеля GRE.	[edit] admin@V2# set interfaces tunnel tun0 remote-ip 203.0.113.1
Указание режима инкапсуляции для туннеля.	[edit] admin@V2# set interfaces tunnel tun0 encapsulation gre
Изменение MTU.	[edit] admin@V2# set interfaces tunnel tun0 mtu 1400
Фиксация настройки.	[edit] admin@V2# commit

Вывод настройки.	[edit]
	admin@V2# show interfaces tunnel tun0
	{
	address 10.0.0.2/30
	encapsulation gre
	local-ip 198.51.100.1
	multicast disable
	mtu 1400
	remote-ip 203.0.113.1
	ttl 255
	}

2.6.2.2. Изменение режима работы ESP

В примере 37 приведено изменение режима работы группы ESP.

В данном примере предполагается, что уже настроена группа ESP с именем ESP-1V.

Пример 37 – Изменение режима работы ESP

Действие	Команда
Изменение режима работы ESP на транспортный режим.	[edit] admin@V2#set vpn ipsec esp-group ESP-1V mode transport
Фиксация изменений	[edit] admin@V2# commit

Вывод настроек группы ESP	[edit]
	admin@V2# show vpn ipsec esp-group ESP-V2
	lifetime 1800
	mode transport
	proposal 1 {
	encryption aes
	hash hmac_sha1
	}
	proposal 2 {
	encryption camellia
	hash hmac_md5
	}

2.6.2.3. Определение настроек IPsec на узле V2

В примере 38 приведено создание туннеля IPsec от узла V2 к узлу V1.

- На узле V2 интерфейсу eth0 назначен IP-адрес 198.51.100.1.
- На узле V1 интерфейсу eth0 назначен IP-адрес 203.0.113.1.
- Используется группа IKE с именем IKE-V2.
- В качестве предварительного ключа используется строка "test_key_1".
- IPsec обеспечивает шифрование между адресом 198.51.100.1 узла V2 и адресом 203.0.113.1 узла V1 и использует группу ESP с именем ESP-V2.

В данном примере предполагается, что уже настроено следующее:

- Группа IKE с именем IKE-V2.
- Группа ESP с именем ESP-V2.

Для создания туннеля IPsec от узла V2 к узлу V1 необходимо выполнить следующие действия на узле V2 в режиме настройки:

Пример 38 – Создание туннеля IPsec от узла V2 к узлу V1

Действие	**Команда**
Определение туннеля в межфилиальном режиме к узлу V1.	`[edit]` `admin@V2# set vpn ipsec site-to-site peer 203.0.113.1`
Переход к другому узлу конфигурации для более удобного редактирования.	`[edit]` `admin@V2# edit vpn ipsec site-to-site peer 203.0.113.1`
Установка режима аутентификации.	`[edit]` `admin@V2# set authentication method pre-shared-key`
Ввод строки, которая будет использоваться для аутентификации узлов.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V2# set authentication pre-shared-key test_key_1`
Указание группы IKE.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V2# set ike-group IKE-V2`
Указание IP-адреса данной системы Numa Edge, который будет использоваться для этого подключения.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V2# set local-ip 198.51.100.1`
Указание IP-адреса удаленного шлюза VPN.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V2# set remote-ip 203.0.113.1`
Указание группы ESP для данного туннеля.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V2# set esp-group ESP-V2`
Возврат к вершине дерева настройки.	`[edit vpn ipsec site-to-site peer 203.0.113.1]` `admin@V2# top`
Фиксация настройки.	`[edit]` `admin@V2# commit`

Вывод настройки.	`[edit]`
	`admin@V2# show vpn ipsec site-to-site peer 203.0.113.1`
	`authentication {`
	`  method pre-shared-key`
	`  pre-shared-key test_key_1`

Действие	Команда
	} esp-group ESP-V2 ike-group IKE-V2 local-ip 198.51.100.1 nat-traversal off remote-ip 203.0.113.1

2.6.2.4. Определение статического маршрута на узле V2

В примере 39 создается статический маршрут до подсети на узле V2 через GRE туннель.

Отправка трафика, предназначенного для подсети 192.168.11.0/24, через туннельный интерфейс tun0. Для создания статического маршрута необходимо выполнить на узле V2 следующие действия в режиме настройки:

Пример 39 – Определение статического маршрута на узле V2

Действие	Команда
Создание статического маршрута	[edit] admin@V2# set protocols static interface-route 192.168.11.0/24 next-hop-interface tun0
Фиксация настройки.	[edit] admin@V2# commit

Вывод настройки.	[edit]
	admin@V2# show protocols static route 192.168.11.0/24 {
	  next-hop-interface tun0
	}

2.7. Узлы VPN, имеющие динамические IP-адреса

В приведенных примерах настройки использовались локальные и удаленные узлы, имеющие статические IP-адреса. Однако они могут иметь динамические IP-адреса. Ниже приведены различные варианты использования с описанием параметров, которые должны быть указаны в каждом их этих случаев (когда локальный и удаленный узлы имеют как статические, так и динамические адреса).

Вариант настройки	Значение параметров
Локальный узел имеет статический IP-адрес	local-ip: IP-адрес локального интерфейса authentication id: @id
Локальный узел имеет динамический IP-адрес	local-ip: 0.0.0.0 authentication id: @id
Удаленный узел имеет статический адрес	remote-ip: IP-адрес удаленного узла authentication remote-id: @id
Удаленный узел имеет динамический IP-адрес	remote-ip: 0.0.0.0 authentication remote-id: @id

3. НАБЛЮДЕНИЕ ЗА СОСТОЯНИЕМ IPSEC VPN В МЕЖФИЛИАЛЬНОМ РЕЖИМЕ

В этом разделе рассматриваются следующие вопросы:

- Вывод сведений IKE.
- Вывод сведений IPSec.
- Отправка сообщений IPSec VPN в системный журнал.
- Фильтрация трафика IPSec.

В данном разделе приведены следующие примеры:

- Пример 40 – Вывод защищенных соединений IKE SA
- Пример 41 – Вывод защищенных соединений IPSec SA
- Пример 42 – Вывод сведений о состоянии IPSec

ПРИМЕЧАНИЕ Вывод, приведенный для данных примеров, может не соответствовать тестовой конфигурации.

3.1. Вывод сведений IKE

Для просмотра IKE SA, используется команда **show vpn ike sa**, как показано в примере ниже.

Пример 40 – Вывод защищенных соединений IKE SA

```
admin@V1:~$ show vpn ike sa

Source           Destination         Cookies                          ST S V E
Created        Phase2

198.51.100.1:500 203.0.113.1:500 fca8e0d08086a0c9:9ddaf66104ebcf36 9 I 10 M
2020-06-02 11:59:34 1
```

3.2. Вывод сведений IPSec

Для просмотра защищенных соединений IPSec SA, используется команда **show vpn ipsec sa**

Пример 41 – Вывод защищенных соединений IPSec SA

```
admin@V1:~$ show vpn ipsec sa
198.51.100.1 203.0.113.1
        esp mode=transport spi=79162189(0x04b7eb4d) reqid=0(0x00000000)
        E: gost-cbc  7878dfd1 56a113fe 89d99c79 fbb6f13c 9cf780d7 1868843c
b408d44f 85002838
        A: hmac-gosthash-2012-256  78473f55 101a0cf2 15f5e07f 2457a5e4
2066ddd6 5a1b040f 737cd18b e065fc5c
        seq=0x00000000 replay=4 flags=0x00000000 state=mature
        created: Jun  2 11:59:35 2020   current: Jun  2 12:17:34 2020
        diff: 1079(s)   hard: 3600(s)   soft: 2880(s)
        last: Jun  2 11:59:36 2020      hard: 0(s)      soft: 0(s)
        current: 512(bytes)     hard: 0(bytes)  soft: 0(bytes)
        allocated: 8    hard: 0 soft: 0
        sadb_seq=1 pid=14961 refcnt=0
203.0.113.1 198.51.100.1
        esp mode=transport spi=33049694(0x01f84c5e) reqid=0(0x00000000)
        E: gost-cbc  1c893e2f f1741515 c3993dbe 3797574f 23762850 182f752c
51c51d4b ee269041
```

```
        A: hmac-gosthash-2012-256  1585c72e 292f5a2f 5184f88e 6ec19621
dc95fdb1 c7ec9f8a 79f8be70 e88104e3
        seq=0x00000000 replay=4 flags=0x00000000 state=mature
        created: Jun  2 11:59:35 2020   current: Jun  2 12:17:34 2020
        diff: 1079(s)   hard: 3600(s)   soft: 2880(s)
        last: Jun  2 11:59:36 2020      hard: 0(s)      soft: 0(s)
        current: 512(bytes)     hard: 0(bytes)  soft: 0(bytes)
        allocated: 8    hard: 0 soft: 0
        sadb_seq=0 pid=14961 refcnt=0
```

Для отображения состояния процесса IPSec, используется команда **show vpn ipsec status**, как показано в примере ниже.

Пример 42 – Вывод сведений о состоянии IPSec

```
admin@V1:~$ show vpn ipsec status
IPsec работает, активных туннелей: 2
```

3.3. Отправка сообщений IPSec VPN в системный журнал

Процесс IPSec генерирует сообщения системного журнала во время исполнения.

Следует учитывать, что в текущей реализации в системный журнал записываются только сообщения с уровнем серьезности **notice** и выше.

Настройка режима регистрации является необязательной. По умолчанию в системный журнал записываются сообщения о запуске и останове IPSec. Режимы регистрации позволяют указать системе проверять пакеты IPSec и регистрировать результат.

Следует учесть, что использование некоторых режимов регистрации может существенно снизить производительность системы.

Для сообщений журнала VPN IPSec используются стандартные уровни серьезности сообщений.

Numa Edge поддерживает следующие режимы регистрации для IPSec VPN.

Таблица 1 – Уровни серьезности сообщений IPSec VPN

Серьезность	Смысл
emerg	Критическая ситуация. Произошел общий сбой системы или другой серьезный сбой, такой что система непригодна для использования.
alert	Уведомление. Необходимо немедленное вмешательство для предотвращения перехода системы в непригодное для использования состояние — например, произошел сбой сети или имел место несанкционированный доступ к базе данных.
crit	Важнейший. Возникло условие максимальной важности, такое как исчерпание ресурсов, — например, в системе отсутствует свободная память, лимиты загрузки ЦП превзойдены или произошёл аппаратный сбой.
err	Ошибка. Возникло условие ошибки, например, произошел сбой системного вызова. Однако система все еще функционирует.
warning	Предупреждение. Произошло событие, которое в принципе может вызвать ошибку, например, передаваемые в функцию недопустимые параметры. За этой ситуацией следует наблюдать.
notice	Замечание. Произошло обычное, но важное событие, такое как непредвиденное событие. Это не ошибка, но оно в принципе может потребовать внимания.
info	Информационное. По мере появления сообщается об обычных событиях, которые могут представлять интерес.
debug	Уровень отладки. Предоставляются сведения уровня отслеживания.

Серьезность	Смысл
all	Все. Предоставляются сведения обо всех уровнях.

ПРЕДОСТЕРЕЖЕНИЕ Есть риск ухудшения качества обслуживания. Уровень серьезности debug требователен к ресурсам. Установка уровня регистрации на debug может вызвать ухудшение функционирования системы.

3.4. Фильтрация трафика IPSec

При применении правил межсетевого экрана для фильтрации трафика IPSec к интерфейсам, необходимо учитывать порядок прохождения пакетов.

Для того чтобы разрешить прохождение трафика IPSec через межсетевой экран, необходимо добавить следующие разрешающие правила на внешнем интерфейсе (подключенному ко внешнему сегменту сети):

- порт источника/назначения UDP с номером 500;
- протокол ESP (номер протокола 50);
- протокол AH (номер протокола 51).

Пакет ESP, отправленный удаленным шлюзом IPSec, принимается на внешнем интерфейсе. В том случае если прохождение этого пакета разрешено, он обрабатывается и расшифровывается. Расшифрованный пакет (имеет адрес отправителя из удаленной сети) попадает на внешний интерфейс и затем обрабатывается в соответствии с правилами межсетевого экрана. Таким образом, необходимо добавить разрешающее правило для прохождения пакетов из заданной подсети на внешнем интерфейсе.

Альтернативным вариантом может являться организация дополнительного слоя туннелирования, например, создание туннеля GRE, в который будет заворачиваться трафик IPSec. В этом случае требуется создать разрешающие правила межсетевого экрана, для прохождения трафика туннеля.

4. КОМАНДЫ IPSEC

В данном разделе приведены следующие команды:

Таблица 2 - Команды IPSec в межфилиальном режиме

Команды настройки	
Общие команды IPSec	
vpn ipsec	Включение IPSec VPN.
vpn ipsec logging	Указание параметров регистрации IPSec VPN.
Группы AH	
vpn ipsec ah-group <имя_группы>	Определение поименованной настройки AH.
vpn ipsec ah-group <имя_группы> hash <алгоритм_хеширования>	Указание алгоритма хеширования, используемого для создания заголовка аутентификации.
Группы ESP	
vpn ipsec esp-group <имя_группы>	Определение поименованной настройки ESP, используемой для согласования второй фазы IKE.
vpn ipsec esp-group <имя_группы> compression <состояние>	Указание того, должен ли данный шлюз VPN предлагать использование сжатия.
vpn ipsec esp-group <имя_группы> lifetime <время_жизни>	Указание времени жизни ключа ESP.
vpn ipsec esp-group <имя_группы> mode <режим>	Указание режима подключения IPSec.
vpn ipsec esp-group <имя_группы> pfs-group <группа>	Определение использования механизма PFS.
vpn ipsec esp-group <имя_группы> proposal <номер>	Определение предложения группы ESP для согласования второй фазы IKE.
vpn ipsec esp-group <имя_группы> proposal <номер> encryption <алгоритм_шифрования>	Определение алгоритма шифрования для указанного предложения группы ESP.
vpn ipsec esp-group <имя_группы> proposal <номер> hash <алгоритм_хеширования>	Определение алгоритма хеширования для указанного предложения группы ESP.
Группа IKE	
vpn ipsec ike-group <имя_группы>	Определение поименованной настройки IKE, используемой для согласования первой фазы IKE.
vpn ipsec ike-group <имя_группы> dead-peer-detection	Определение поведения системы в том случае, если узел VPN становится недоступен.
vpn ipsec ike-group <имя_группы> lifetime <время_жизни>	Указание времени жизни ключа IKE.
vpn ipsec ike-group <имя_группы> proposal <номер>	Определение предложения группы IKE для согласования первой фазы IKE.
vpn ipsec ike-group <имя_группы> proposal <номер> dh-group <группа>	Указание группы Oakley, которая будет предложена для ключевого обмена Диффи-Хеллмана.

vpn ipsec ike-group <имя_группы> proposal <номер> encryption <алгоритм_шифрования>	Определение алгоритма шифрования для указанного предложения группы IKE.
vpn ipsec ike-group <имя_группы> proposal <номер> hash <алгоритм_хеширования>	Определение алгоритма хеширования для указанного предложения группы IKE.
Туннель IPSec	
vpn ipsec site-to-site peer <туннель>	Определение подключения в межфилиальном режиме между системой Numa Edge и другим шлюзом VPN.
vpn ipsec site-to-site peer <туннель> authentication	Предоставление сведений, необходимых для аутентификации.
vpn ipsec site-to-site peer <туннель> ah-group <имя_группы>	Указание группы AH, используемой для данного туннеля.
vpn ipsec site-to-site peer <туннель> esp-group <имя_группы>	Указание поименованной настройки ESP, которая будет использована при подключении к данному узлу.
vpn ipsec site-to-site peer <туннель> ike-group <имя_группы>	Указание поименованной настройки IKE, которая будет использована при подключении к данному узлу.
vpn ipsec site-to-site peer <туннель> local-ip <ipv4-адрес>	Указание локального IP-адреса, который будет использоваться в качестве IP-адреса отправителя для пакетов, предназначенных удаленному узлу.
vpn ipsec site-to-site peer <туннель> remote-ip <ipv4-адрес>	Указание IP-адреса удаленного шлюза VPN.
vpn ipsec site-to-site peer <туннель> local-subnet <ipv4-сеть>	Указание адреса локальной сети, расположенной за данным шлюзом VPN.
vpn ipsec site-to-site peer <туннель> remote-subnet <ipv4-сеть>	Указание адреса удаленной сети, расположенной за удаленным шлюзом VPN.
vpn ipsec site-to-site peer <туннель> nat-traversal <состояние>	Определение использования технологии NAT-T на локальном устройстве.
Эксплуатационные команды	
clear vpn ipsec-peer <туннель>	Перезапуск туннелей, ассоциированных с указанным узлом IPSec.
clear vpn ipsec-process	Перезапуск процесса IPSec.
show vpn ike rsa-keys	Отображение ключей RSA, о которых есть запись в системе.
show vpn ike sa	Вывод сведений обо всех активных в данный момент защищенных соединениях IKE (ISAKMP).
show vpn ike secrets	Вывод настроенных предварительных ключей.
show vpn ipsec sa	Вывод сведений обо всех активных в данный момент защищенных соединений IPSec.
show vpn ipsec status	Вывод сведений о состоянии процессов IPSec.
Управление RSA ключами	
vpn rsa-keys delete <имя_ключа>	Удаление ключевой пары RSA из системного хранилища.

vpn rsa-keys export <имя_ключа> to <имя_файла>	Экспорт открытого ключа из ключевой пары, используемого на другом устройстве для установки соединения.
vpn rsa-keys generate <имя_ключа> bits <размер>	Генерация файла, содержащего ключевую пару RSA.
vpn rsa-keys import <имя_ключа> from <имя_файла>	Импорт открытого ключа RSA в системное хранилище.
vpn rsa-keys list	Просмотр файлов RSA ключей в системном хранилище.

4.1. Команды настройки

4.1.1. vpn ipsec

Включение IPSec VPN в системе Numa Edge.

Синтаксис

```
set vpn ipsec
delete vpn ipsec
show vpn ipsec
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
   }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет включить IPSec VPN в системе Numa Edge.

ПРИМЕЧАНИЕ Отправка и получение сообщений ICMP о перенаправлении отключена при использовании IPSec VPN.

Форма **set** данной команды используется для включения IPSec VPN.

Форма **delete** используется для удаления всей настройки IPSec VPN и отключения IPSec VPN.

Форма **show** данной команды используется для отображения настройки IPSec VPN.

4.1.2. vpn ipsec logging

Указание параметров регистрации IPSec VPN.

Синтаксис

```
set vpn ipsec logging [log-modes <режим>]
delete vpn ipsec logging [log-modes]
show vpn ipsec logging [log-modes]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      logging {
         log-modes режим
      }
   }
}
```

Параметры

режим

Обязательный. Множественный узел. Режим регистрации, используемый для регистрационных сообщений IPSec. Поддерживаются следующие значения:

- debug;
- debug2;
- error;
- info;
- notify;
- warning.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания уровня серьезности сообщений регистрации IPSec VPN. Чем ниже указанный уровень серьезности, тем более подробная информация будет записана в файл журнала.

Процесс IPSec генерирует сообщения регистрации во время исполнения, которые могут быть направлены в системный журнал.

Следует учитывать, что в текущей реализации в главном файле журнала регистрируются только сообщения с уровнем серьезности **notice** и выше.

Настройка режима регистрации является необязательной. В том случае если режим регистрации явно не указан, генерируются сообщения регистрации IPSec с уровнем серьезности **info**, к которым относятся в основном сообщения о запуске и остановке IPSec.

Следует учесть, что использование некоторых режимов регистрации может существенно снизить производительность системы.

Для регистрационных сообщений VPN IPSec используются стандартные уровни серьезности, используемые в syslog.

Форма **set** данной команды используется для указания режима регистрации для IPSec VPN.

Форма **delete** данной команды используется для удаления настройки регистрации.

Форма **show** данной команды используется для отображения настройки регистрации.

4.2. Группы AH

4.2.1. vpn ipsec ah-group <имя_группы>

Определение поименованной настройки AH.

Синтаксис

```
set vpn ipsec ah-group <имя_группы>
delete vpn ipsec ah-group
show vpn ipsec ah-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
    ah-group имя_группы {
      }
   }
}
```

Параметры

имя_группы

Множественный узел. Имя, используемое для обозначения настройки АН.

Можно определить несколько настроек АН, создав соответствующее количество узлов конфигурации **ah-group**.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для создания группы АН.

Группа АН позволяет задать параметры АН (Authentication Header).

Форма **set** данной команды используется для создания и изменения группы АН.

Форма **delete** данной команды используется для удаления настройки группы АН.

Форма **show** данной команды используется для отображения настройки группы АН.

4.2.2. vpn ipsec ah-group <имя_группы> hash <алгоритм_хеширования>

Указание алгоритма хеширования, используемого для создания заголовка аутентификации.

Синтаксис

```
set vpn ipsec ah-group <имя_группы> hash <алгоритм_хеширования>
delete vpn ipsec ah-group hash
show vpn ipsec ah-group hash
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      ah-group имя_группы {
         hash алгоритм_шифрования
      }
   }
}
```

Параметры

имя

Имя, используемое для обозначения настройки АН.

алгоритм_хеширования

Используемый алгоритм хеширования. Поддерживаются следующие значения:

- des;
- 3des;
- des_iv64;

- des_iv32;
- hmac_sha1;
- hmac_sha512;
- hmac_gosthash;
- hmac_gosthash-2012-256;
- hmac_gosthash-2012-512;
- hmac_gosthash-st;
- hmac_gosthash-zstv;
- hmac_sha256;
- non_auth;
- hmac_md5;
- hmac_sha384.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания алгоритма хеширования, который будет использован для создания заголовка аутентификации.

Numa Edge поддерживает российский криптографический стандарт вычисления хеш-функции ГОСТ Р34.11-94 (**hmac_gosthash**) и ГОСТ Р34.11-2012 **(hmac_gosthash-2012)**.

ПРИМЕЧАНИЕ При использовании для аутентификации протокола AH в настройке группы ESP для параметра **vpn ipsec esp-group <имя_группы> proposal <номер> hash** должно быть установлено значение **no_auth.**

Форма **set** данной команды позволяет указать алгоритм хеширования, который будет предложен к использованию.

Форма **delete** данной команды используется для восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки алгоритма хеширования.

4.3. Группа ESP

4.3.1. vpn ipsec esp-group <имя_группы>

Определение поименованной настройки ESP для соглашений второй фазы IKE.

Синтаксис

```
set vpn ipsec esp-group <имя_группы>
delete vpn ipsec esp-group
show vpn ipsec esp-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      esp-group имя_группы {
      }
   }
}
```

Параметры

имя_группы

Множественный узел. Имя, используемое для обозначения настройки ESP.Можно определить несколько настроек ESP, создав соответствующее количество узлов конфигурации **esp-group**. По крайней мере одна настройка ESP должна быть определена для использования в настройке туннеля.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для создания группы ESP.

Группа ESP позволяет задать параметры ESP (Encapsulating Security Payload), которые необходимы для второй фазы IKE, а также для установки времени жизни защищенного соединения IPSec (SA).

Форма **set** данной команды используется для создания и изменения группы ESP.

Форма **delete** данной команды используется для удаления настройки группы ESP.

Форма **show** данной команды используется для отображения настройки группы ESP.

4.3.2. vpn ipsec esp-group <имя_группы> compression <состояние>

Указание того, должен ли данный шлюз VPN предлагать использование сжатия.

Синтаксис

```
set vpn ipsec esp-group <имя_группы> compression <состояние>
delete vpn ipsec esp-group <имя_группы> compression
show vpn ipsec esp-group <имя_группы> compression
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      esp-group имя_группы {
         compression состояние
      }
   }
}
```

Параметры

имя_группы

Имя, используемое для обозначения настройки ESP.

состояние

Включение/отключение сжатия ESP. Поддерживаемые значения:

- **enable**: Включение предложения сжатия ESP.
- **disable**: Отключение предложения сжатия ESP.

Значение по умолчанию

Сжатие ESP отключено.

Указания по использованию

Данная команда позволяет установить, следует ли включать в предложение сжатие ESP при согласовании второй фазы IKE.

Форма **set** данной команды используется для включения/отключения сжатия ESP.

Форма **delete** используется для восстановления поведения по умолчанию.

Форма **show** данной команды используется для отображения настройки сжатия ESP.

4.3.3. vpn ipsec esp-group <имя_группы> lifetime <время_жизни>

Указание времени жизни ключа ESP.

Синтаксис

```
set vpn ipsec esp-group <имя_группы> lifetime <время_жизни>
delete vpn ipsec esp-group <имя_группы> lifetime
show vpn ipsec esp-group <имя_группы> lifetime
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      esp-group имя_группы {
         lifetime время жизни
      }
   }
}
```

Параметры

имя_группы

Имя, используемое для обозначения настройки ESP.

время_жизни

Время, в секундах, в течение которого ключ, созданный при согласовании второй фазы IKE, остается в силе. Значение должно лежать в диапазоне от 30 до 86400 (что соответствует 24 часам). По умолчанию используется значение 3600.

Значение по умолчанию

Ключ остается действующим в течение 3600 секунд (1 час).

Указания по использованию

Данная команда позволяет указать время жизни ключа.

Форма **set** данной команды используется для указания времени жизни ключа.

Форма **delete** данной команды используется для удаления настройки времени жизни ключа.

Форма **show** данной команды используется для отображения настройки времени жизни ключа.

4.3.4. vpn ipsec esp-group <имя_группы> mode <режим>

Указание режима подключения IPSec.

Синтаксис

```
set vpn ipsec esp-group <имя_группы> mode <режим>
delete vpn ipsec esp-group <имя_группы> mode
show vpn ipsec esp-group <имя_группы> mode
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      esp-group имя_группы {
         mode режим
      }
   }
}
```

Параметры

имя_группы

Имя, используемое для обозначения настройки ESP.

режим

Режим подключения IPSec. Поддерживаемые значения:

- **tunnel**: Туннельный режим.
- **transport**: Транспортный режим.

Значение по умолчанию

Используется туннельный режим.

Указания по использованию

Данная команда позволяет установить режим подключения IPSec.

Форма **set** данной команды используется для указания используемого режима IPSec.

Форма **delete** данной команды используется для восстановления режима подключения IPSec.

Форма **show** данной команды используется для отображения настройки режима подключения IPSec.

4.3.5. vpn ipsec esp-group <имя_группы> pfs-group <группа>

Определение использования механизма PFS.

Синтаксис

```
set vpn ipsec esp-group <имя_группы> pfs-group <группа>
delete vpn ipsec esp-group <имя_группы> pfs-group
show vpn ipsec esp-group <имя_группы> pfs-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      esp-group имя_группы {
         pfs-group группа
      }
   }
}
```

Параметры

имя_группы

Имя, используемое для обозначения настройки ESP.

группа

Включение/отключение PFS (Perfect Forward Secrecy). Поддерживаемые значения:

- **2**: Использовать группу Диффи-Хеллмана 2.
- **5**: Использовать группу Диффи-Хеллмана 5.

Значение по умолчанию

Использование PFS по умолчанию отключено.

Указания по использованию

Данная команда позволяет включить/отключить PFS (Perfect Forward Secrecy).

Помимо использования ключевого обмена Диффи-Хеллмана в первой фазе установления соединения IPSec можно также использовать его во второй фазе, включив PFS при помощи данной команды. При использовании PFS ключ, используемый для защиты передаваемых данных, не должен использоваться для получения любых дополнительных ключей, и если ключ,

используемый для защиты передаваемых данных, был получен из некоторого другого ключевого материала, то этот ключевой материал не должен больше использоваться для получения других ключей. Группа Диффи-Хеллмана, которая указывается при включении PFS, определяет стойкость используемого ключа. Чем выше номер группы, тем более стойкие ключи используются, однако это также приводит к увеличению используемых вычислительных ресурсов. При использовании PFS во второй фазе обмен Диффи-Хеллмана происходит каждый раз при установлении IPSec SA. Группа Диффи-Хеллмана, выбранная для фазы 2, может не совпадать с группой Диффи-Хеллмана, выбранной для фазы 1.

Форма **set** данной команды позволяет включить/отключить PFS (Perfect Forward Secrecy).

Форма **delete** данной команды используется для восстановления настройки PFS, используемой по умолчанию.

Форма **show** данной команды используется для отображения настройки PFS.

4.3.6. vpn ipsec esp-group <имя_группы> proposal <номер>

Определение предложения группы ESP для согласования второй фазы IKE.

Синтаксис

```
set vpn ipsec esp-group <имя_группы> proposal <номер>
delete vpn ipsec esp-group <имя_группы> proposal
show vpn ipsec esp-group <имя_группы> proposal
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      esp-group имя_группы {
         proposal номер {
         }
       }
   }
}
```

Параметры

имя_группы

Имя, используемое для обозначения настройки ESP.

номер

Множественный узел. Целое число, уникально идентифицирующее предложение, используемое при согласовании второй фазы IKE. Можно определить несколько предложений, относящихся к одной группы ESP, создав соответствующее количество узлов конфигурации **proposal**. Каждое предложение должно иметь уникальный идентификатор.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для определения предложения ESP для согласования второй фазы IKE.

Форма **set** данной команды используется для создания предложения ESP.

Форма **delete** данной команды используется для удаления предложения ESP и его настройки.

Форма **show** данной команды используется для отображения настройки предложения ESP.

4.3.7. vpn ipsec esp-group <имя_группы> proposal <номер> encryption

<алгоритм_шифрования>

Указание алгоритма шифрования для предложения ESP.

Синтаксис

```
set vpn ipsec esp-group <имя_группы> proposal <номер>
encryption <алгоритм_шифрования>
delete vpn ipsec esp-group proposal <номер> encryption
show vpn ipsec esp-group proposal <номер> encryption
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      esp-group имя_группы {
         proposal номер {
            ecnryption алгоритм_шифрования
         }
       }
   }
}
```

Параметры

имя_группы

Имя, используемое для обозначения настройки ESP.

номер

Целое число, уникально идентифицирующее предложение, используемое при согласовании второй фазы IKE.

алгоритм_шифрования

Алгоритм шифрования, который будет предложен. Поддерживаются следующие значения:

- blowfish;
- cast128;
- gost;
- gost-zstv;
- twofish;
- aes;
- camellia;
- null_enc;
- rijndael.

Значение по умолчанию

По умолчанию установлено значение **aes**.

Указания по использованию

Данная команда используется для указания алгоритма шифрования, который будет предложен при согласовании второй фазы IKE в рамках указанного предложения ESP. Numa Edge поддерживает российский стандарт симметричного шифрования ГОСТ 28147-89 (**gost**).

Форма **set** данной команды используется для указания алгоритма шифрования.

Форма **delete** данной команды используется для восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки алгоритма шифрования в предложении ESP.

4.3.8. vpn ipsec esp-group <имя_группы> proposal <номер> hash <алгоритм_хеширования>

Указание алгоритма хеширования для предложения ESP.

Синтаксис

```
set vpn ipsec esp-group <имя_группы> proposal <номер>
hash <алгоритм_хеширования>
delete vpn ipsec esp-group <имя_группы> proposal <номер> hash
show vpn ipsec esp-group <имя_группы> proposal <номер> hash
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      esp-group имя_группы {
         proposal номер {
            ecnryption алгоритм_хеширования
         }
       }
   }
}
```

Параметры

имя_группы

Имя, используемое для обозначения настройки ESP.

номер

Целое число, уникально идентифицирующее предложение, используемое при согласовании второй фазы IKE.

алгоритм_хеширования

Используемый алгоритм хеширования. Поддерживаются следующие значения:

- hmac_sha1;
- hmac_sha512;
- hmac_gosthash;
- hmac_gosthash-2012-256;
- hmac_gosthash-2012-512;
- hmac_gosthash-zstv;
- hmac_gosthash-st;
- hmac_sha256;
- non_auth;
- hmac_md5;
- hmac_sha384.

Значение по умолчанию

По умолчанию установлено значение **sha1**.

Указания по использованию

Данная команда используется для указания алгоритма хеширования, который будет предложен в рамках предложения ESP.

Numa Edge поддерживает российский криптографический стандарт вычисления хеш-функции ГОСТ Р 34.11-94 (**hmac_gosthash**) и ГОСТ Р 34.11-2012 **(hmac_gosthash-2012)**.

ПРИМЕЧАНИЕ При использовании для аутентификации протокола AH для данного параметра необходимо установить значение **no_auth**. Алгоритм хеширования используемый для аутентификации в этом случае указывается при помощи команды **vpn ipsec ah-group <имя_группы> hash <алгоритм_хеширования>** (см. стр.62).

Форма **set** данной команды позволяет указать алгоритм хеширования, который будет предложен к использованию.

Форма **delete** данной команды используется для восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки алгоритма хеширования, указанного в предложении ESP.

4.4. Группа IKE

4.4.1. vpn ipsec ike-group <имя_группы>

Определение поименованной настройки IKE для согласований первой фазы IKE.

Синтаксис

```
set vpn ipsec ike-group <имя_группы>
delete vpn ipsec ike-group
show vpn ipsec ike-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      ike-group имя_группы {
      }
   }
}
```

Параметры

имя_группы

Обязательный. Множественный узел. Имя, используемое для обозначения настройки IKE.

Можно создать множественные настройки IKE, создав соответствующее количество узлов конфигурации **ike-group**.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для определения набора параметров настройки IKE.

Данная настройка IKE может быть использована при настройке туннеля к узлу VPN с использованием команды **vpn ipsec site-to-site peer <туннель>** (см. стр. 76).

Форма **set** данной команды используется для создания группы IKE. Форма **delete** данной команды используется для удаления группы IKE и ее настройки.

Форма **show** данной команды используется для отображения настройки группы IKE.

4.4.2. vpn ipsec ike-group <имя_группы> dead-peer-detection

Определяет поведение системы в том случае, если узел VPN становится недоступен.

Синтаксис

```
set vpn ipsec ike-group <имя_группы> dead-peer-detection
[interval <интервал> | timeout <таймаут>]
delete vpn ipsec ike-group <имя_группы> dead-peer-detection
```

```
show vpn ipsec ike-group <имя_группы> dead-peer-detection
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      ike-group имя_группы {
         dead-peer-detection {
            interval интервал
            timeout таймаут
         }
      }
   }
}
```

Параметры

имя_группы

Имя, используемое для обозначения настройки IKE.

интервал

Интервал времени, в секундах, через который узлам VPN будут отправляться сообщения IKE, подтверждающие активность (keep-alive messages). Значение должно лежать в диапазоне от 15 до 86400. По умолчанию установлено значение 30.

таймаут

Интервал времени, в секундах, по истечении которого, в том случае если узел не отвечает, осуществляется попытка перезапуска туннеля. Значение должно лежать в диапазоне от 30 до 86400. По умолчанию установлено значение 120.

Значение по умолчанию

Активность узлов VPN не проверяется.

Указания по использованию

Данная команда определяет то, каким образом должны отслеживаться неактивные узлы IPSec VPN.

Форма **set** данной команды используется для определения отслеживания узлов, ставших неактивными.

Форма **delete** данной команды используется для удаления настройки отслеживания неактивных узлов VPN.

Форма **show** данной команды используется для отображения настройки.

4.4.3. vpn ipsec ike-group <имя_группы> lifetime <время_жизни>

Указание времени жизни ключа IKE.

Синтаксис

```
set vpn ipsec ike-group <имя_группы> lifetime <время_жизни>
delete vpn ipsec ike-group <имя_группы> lifetime
show vpn ipsec ike-group <имя_группы> lifetime
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      ike-group имя_группы {
         lifetime время_жизни
```

```
        }
    }
}
```

Параметры

имя_группы

Имя, используемое для обозначения настройки IKE.

время_жизни

Время, в секундах, в течение которого ключ, созданный при согласовании первой фазы IKE, остается в силе, до того как будет инициировано новое согласование. Значение должно лежать в диапазоне от 30 до 86400 (что соответствует 24 часам). По умолчанию используется значение 28800 (8 часов).

Значение по умолчанию

Ключ IKE используется в течение 8 часов.

Указания по использованию

Данная команда позволяет указать время жизни для ключа IKE. Форма **set** данной команды используется для указания времени жизни ключа.

Форма **delete** данной команды используется для восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки времени жизни.

4.4.4. vpn ipsec ike-group <имя_группы> proposal <номер>

Указание номера предложения группы IKE.

Синтаксис

```
set vpn ipsec ike-group <имя_группы> proposal <номер>
delete vpn ipsec ike-group <имя_группы> proposal
show vpn ipsec ike-group <имя_группы> proposal
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      ike-group имя_группы {
         proposal номер {
         }
      }
   }
}
```

Параметры

имя_группы

Имя, используемое для обозначения настройки IKE.

номер

Множественный узел. Целое число, уникально идентифицирующее предложение IKE.

Можно определить до 10 предложений в рамках одной группы IKE, создав соответствующее количество узлов конфигурации **proposal**. Каждое предложение должно иметь уникальный идентификатор.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для создания предложения IKE. Данное предложения будет использовано при согласовании первой фазы IKE.

Форма **set** данной команды используется для создания предложения IKE.

Форма **delete** данной команды используется для удаления предложения IKE и его настройки.

Форма **show** данной команды используется для отображения настройки предложения IKE.

4.4.5. vpn ipsec ike-group <имя_группы> proposal <номер> dh-group <группа>

Указание группы Oakley, которая будет предложена для ключевого обмена Диффи-Хеллмана.

Синтаксис

```
set vpn ipsec ike-group <имя_группы> proposal <номер> dh-
group <группа>
delete vpn ipsec ike-group <имя_группы> proposal <номер> dh-group
show vpn ipsec ike-group <имя_группы> proposal <номер> dh-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      ike-group имя_группы {
         proposal номер {
            dh-group группа
         }
      }
   }
}
```

Параметры

имя_группы

Имя, используемое для обозначения настройки IKE.

номер

Целое число, уникально идентифицирующее предложение IKE.

группа

Группа Oakley, используемая при ключевом обмене Диффи-Хеллмана. Поддерживаются следующие значения:

- **2**: Группа Oakley 2.
- **5**: Группа Oakley 5.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания группы Oakley, использование которой будет предлагаться для ключевого обмена Диффи-Хеллмана.

Форма **set** данной команды используется для указания группы Oakley.

Форма **delete** данной команды используется для удаления настройки группы Oakley.

Форма **show** данной команды используется для отображения настройки группы Oakley.

4.4.6. vpn ipsec ike-group <имя_группы> proposal <номер> encryption <алгоритм_шифрования>

Указание алгоритма шифрования, использование которого будет предлагаться при согласовании первой фазы IKE.

Синтаксис

```
set vpn ipsec ike-group <имя_группы> proposal <номер>
encryption <алгоритм_шифрования>
delete vpn ipsec ike-group <имя_группы> proposal <номер> encryption
show vpn ipsec ike-group <имя_группы> proposal <номер> encryption
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      ike-group имя_группы {
         proposal номер {
            encryption алгоритм_шифрования
         }
      }
   }
}
```

Параметры

имя_группы

Имя, используемое для обозначения настройки IKE.

номер

Целое число, уникально идентифицирующее предложение IKE.

алгоритм_шифрования

Алгоритм шифрования, используемый при согласовании первой фазы IKE. Поддерживаются следующие значения:

- aes;
- blowfish;
- camellia;
- cast128;
- gost;
- gost-zstv;
- gost-cbc.

Значение по умолчанию

По умолчанию установлено значение **aes**.

Указания по использованию

Данная команда используется для указания алгоритма шифрования, который будет предложен при согласовании первой фазы IKE.

Numa Edge поддерживает российский стандарт симметричного шифрования ГОСТ 28147-89 (**gost**).

Форма **set** данной команды используется для указания алгоритма шифрования.

Форма **delete** используется для восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки алгоритма шифрования.

4.4.7. vpn ipsec ike-group <имя_группы> proposal <номер> hash <алгоритм_хеширования>

Указание алгоритма хеширования для предложения.

Синтаксис

```
set vpn ipsec ike-group <имя_группы> proposal <номер>
hash <алгоритм_хеширования>
delete vpn ipsec ike-group <имя_группы> proposal <номер> hash
show vpn ipsec ike-group <имя_группы> proposal <номер> hash
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      ike-group имя_группы {
         proposal номер {
            hash алгоритм_хеширования
         }
      }
   }
}
```

Параметры

имя_группы

Имя, используемое для обозначения настройки IKE.

номер

Целое число, уникально идентифицирующее предложение IKE.

алгоритм_хеширования

Используемый алгоритм хеширования.

Поддерживаемые значения:

- gosthash-94;
- gosthash-94-st;
- gosthash-94-zstv;
- gosthash-2012-256;
- gosthash-2012-512;
- md5;
- sha1;
- sha256;
- sha384;
- sha512.

Значение по умолчанию

По умолчанию установлено значение **gosthash-2012-256**.

Указания по использованию

Данная команда используется для указания алгоритма хеширования, который будет предложен к использованию в рамках предложения IKE.

Форма **set** данной команды позволяет указать алгоритм хеширования, который будет предложен к использованию.

Форма **delete** данной команды используется для восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки алгоритма хеширования.

4.5. Туннель IPSec

4.5.1. vpn ipsec site-to-site peer <туннель>

Определение подключения в межфилиальном режиме между системой Numa Edge и другим шлюзом VPN.

Синтаксис

```
set vpn ipsec site-to-site peer <туннель>
delete vpn ipsec site-to-site peer <туннель>
show vpn ipsec site-to-site peer <туннель>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
   ipsec {
      site-to-site {
         peer туннель {
         }
      }
   }
}
```

Параметры

туннель

Множественный. Название туннеля к удаленному узлу IPSec.

Можно создать несколько туннелей VPN, создав соответствующее количество узлов конфигурации **peer**.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для определения туннеля к другому узлу VPN в межфилиальном режиме, обеспечивающего взаимодействие между подсетью, расположенной за локальным шлюзом VPN (**local-subnet**), и подсетью, расположенной за удаленным шлюзом VPN (**remote-subnet**). Для настройки нескольких туннелей необходимо создать соответствующее количество узлов конфигурации **peer**.

Форма **set** данной команды используется для определения туннеля в межфилиальном режиме к другому узлу VPN.

Форма **delete** данной команды используется для удаления настройки туннеля.

Форма **show** данной команды используется для отображения настройки туннеля.

4.5.2. vpn ipsec site-to-site peer <туннель> authentication

Указание сведений, необходимых для аутентификации.

Синтаксис

```
set vpn ipsec site-to-site peer <туннель> authentication [id <id> |
key <ключ>| method <метод> | peer-id <id> | peer-key <key> | pre-
shared-key <key> | verify-id <режим> | x509-cert <сертификат>]
delete vpn ipsec site-to-site peer <туннель> authentication [id | key
| method | peer-id | peer-key | pre-shared-key | verify-id | x509-
cert]
show vpn ipsec site-to-site peer <туннель> authentication [id | key |
method | peer-id | peer-key | pre-shared-key | verify-id | x509-cert]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
   ipsec {
      site-to-site {
         peer туннель {
            authentication {
               id id
               key ключ
               method метод
               peer-id id
               pre-shared-key ключ
               verify-id режим
               x509-cert сертификат
            }
         }
      }
   }
}
```

Параметры

peer *туннель*

Обязательный. Название туннеля к удаленному узлу IPSec.

id *id*

Идентификационные данные локального узла VPN, которые будут предъявляться удаленному узлу VPN. Значение указывается в следующем формате: @идентификатор.

key *имя*

Имя ключевой пары RSA для локального узла VPN. Для генерации ключевой пары RSA используется команда **vpn rsa-keys generate** <*key*>. Далее, полученное значение <*key*> ключевой пары используется для данного параметра. Указание значения является обязательным при использовании аутентификации на основе криптосистемы RSA (**authentication method plain-rsa**).

method *метод*

Указание режима аутентификации, используемого для данного туннеля. Поддерживаются следующие значения:

- **pre-shared-key**: Использование предварительных ключей для аутентификации.
- **plain-rsa**: Использование криптосистемы RSA для аутентификации.
- **x509/x509-zstv**: Использование инфраструктуры открытых ключей (PKI) для аутентификации.

peer-id id

Идентификационные данные удаленного узла VPN. Значение указывается в следующем формате: @*идентификатор*. Аутентификация на основе идентификационных данных используется в том случае, если узел VPN имеет динамический адрес.

peer-key имя

Имя открытого ключа RSA удаленного узла VPN. Для записи в систему открытого ключа RSA удаленного узла используется команда **vpn rsa-keys import** <*key*>. Далее, импортированное значение <*key*> открытого ключа используется для данного параметра. Указание значения для данного параметра является обязательным при использовании аутентификации на основе криптосистемы RSA (**authentication method plain-rsa**).

pre-shared-key ключ

Обязательный, если в качестве режима аутентификации установлен режим **pre-shared-key**; в остальных случаях игнорируется. Указание предварительного ключа, используемого для аутентификации удаленного узла.

verify-id режим

Обязательный. Параметр может принимать значение on или off, что позволяет включить или выключить проверку ID удаленного узла IPSec.

x509-cert *имя_сертификата*

Имя сертификата X.509 локального узла VPN. Указание значения для данного параметра является обязательным при использовании аутентификации на основе криптосистемы RSA (**authentication method x509**).

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания сведений, необходимых для аутентификации.

Форма **set** данной команды используется для указания сведений аутентификации.

Форма **delete** данной команды используется для удаления настройки аутентификации для узла IPSec.

Форма **show** данной команды используется для отображения настройки аутентификации для узла IPSec.

4.5.3. vpn ipsec site-to-site peer <туннель> ah-group <имя_группы>

Указание группы AH, используемой для данного туннеля.

Синтаксис

```
set vpn ipsec site-to-site peer <туннель> ah-group <имя_группы>
delete vpn ipsec site-to-site peer <туннель> ah-group
show vpn ipsec site-to-site peer <туннель> ah-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      site-to-site {
         peer туннель {
            ah-group имя_группы
         }
      }
   }
}
```

Параметры

туннель

Обязательный. Название туннеля к удаленному узлу IPSec.

имя_группы

Обязательный. Указание поименованной настройки AH, которая будет использована для данного туннеля. Группа AH должна быть заранее определена с использованием команды **vpn ipsec ah-group <имя_группы>** (см. стр. 60).

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания группы AH, которая будет использована для указанного туннеля.

Форма **set** данной команды используется для указания группы AH.

Форма **delete** данной команды используется для удаления настройки группы AH, используемой для указанного туннеля.

Форма **show** данной команды используется для отображения настройки используемой группы AH.

4.5.4. vpn ipsec site-to-site peer <туннель> esp-group <имя_группы>

Указание группы ESP, используемой для данного туннеля.

Синтаксис

```
set vpn ipsec site-to-site peer <туннель> esp-group <имя_группы>
delete vpn ipsec site-to-site peer <туннель> esp-group
show vpn ipsec site-to-site peer <туннель> esp-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      site-to-site {
         peer туннель {
            esp-group имя_группы
         }
      }
   }
}
```

Параметры

туннель

Обязательный. Название туннеля к удаленному узлу IPSec.

имя_группы

Обязательный. Указание поименованной настройки ESP, которая будет использована для данного туннеля. Группа ESP должна быть заранее определена с использованием команды **vpn ipsec esp-group <имя_группы>** (см. стр. 63).

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания группы ESP, которая будет использована для указанного туннеля.

Форма **set** данной команды используется для указания группы ESP.

Форма **delete** данной команды используется для удаления настройки группы ESP, используемой для указанного туннеля.

Форма **show** данной команды используется для отображения настройки используемой группы ESP.

4.5.5. vpn ipsec site-to-site peer <туннель> ike-group <имя_группы>

Указание поименованной настройки IKE, которая будет использована при подключении к данному узлу.

Синтаксис

```
set vpn ipsec site-to-site peer <туннель> ike-group <имя_группы>
delete vpn ipsec site-to-site peer <туннель> ike-group
show vpn ipsec site-to-site peer <туннель> ike-group
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      site-to-site {
         peer туннель {
            ike-group имя_группы
         }
      }
   }
}
```

Параметры

туннель

Обязательный. Название туннеля к удаленному узлу IPSec.

имя_ируппы

Обязательный. Поименованная настройка IKE, используемая для данного туннеля. Настройка IKE должна быть заранее определена при помощи команды **vpn ipsec ike-group <имя_группы>** (см. стр. 70).

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания поименованной настройки IKE (группы IKE), используемой для данного туннеля.

Форма **set** используется для указания группы IKE.

Форма **delete** данной команды используется для удаления настройки группы IKE.

Форма **show** данной команды используется для отображения настройки группы IKE.

4.5.6. vpn ipsec site-to-site peer <туннель> local-ip <ipv4-адрес>

Указание локального IP-адреса, который будет использоваться в качестве IP-адреса отправителя для пакетов, предназначенных удаленному узлу.

Синтаксис

```
set vpn ipsec site-to-site peer <туннель> local-ip <ipv4-адрес>
delete vpn ipsec site-to-site peer <туннель> local-ip
show vpn ipsec site-to-site peer <туннель> local-ip
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      site-to-site {
         peer туннель {
            local-ip ipv4-адрес
         }
      }
   }
```

```
}
```

Параметры

туннель

Обязательный. Название туннеля к удаленному узлу IPSec.

ipv4-адрес

Обязательный. Локальный IP-адрес, используемый в качестве IP-адреса отправителя для пакетов, предназначенных удаленному узлу.

Также следует учесть:

- Если в целях повышения надежности и отказоустойчивости используется кластеризация, в качестве значения для параметра **local-ip** должен быть указан IP-адрес кластера, а не IP-адрес, назначенный физическому интерфейсу.
- В остальных случаях в качестве значения для параметра **local-ip** должен быть указан IP-адрес, назначенный физическому интерфейсу.
- В том случае если локальный узел имеет динамический IP-адрес значение для параметра **local-ip** не указывается, при этом с помощью команды **vpn ipsec site-to-site peer** <*туннель*> **authentication** должны быть указаны идентификационные данные (см. стр.76).

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания локального IP-адреса, используемого в качестве IP-адреса пакетов, предназначенных для удаленного узла.

В том случае если локальный узел имеет динамический IP-адрес, параметр **local-ip** не используется, в этом случае должны быть указаны идентификационные данные при помощи команды **vpn ipsec site-to-site peer <***туннель***> authentication**.

Форма **set** данной команды используется для указания локального IP-адреса, используемого в качестве адреса отправителя для пакетов, предназначенных удаленному узлу.

Форма **delete** данной команды используется для удаления настройки локального IP-адреса.

Форма **show** данной команды используется для настройки локального IP-адреса.

4.5.7. vpn ipsec site-to-site peer <туннель> remote-ip <ipv4-адрес>

Указание IP-адреса удаленного шлюза.

Синтаксис

```
set vpn ipsec site-to-site peer <туннель> remote-ip <ipv4-адрес>
delete vpn ipsec site-to-site peer <туннель> remote-ip
show vpn ipsec site-to-site peer <туннель> remote-ip
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      site-to-site {
         peer туннель {
            remote-ip ipv4-адрес
         }
      }
   }
}
```

Параметры

туннель

Обязательный. Название туннеля к удаленному узлу IPSec.

ipv4-адрес

Обязательный. IP-адрес удаленного шлюза VPN.

Также следует учесть:

- Если в целях повышения надежности и отказоустойчивости используется кластеризация, в качестве значения для параметра **remote-ip** должен быть указан IP-адрес кластера, а не IP-адрес, назначенный физическому интерфейсу.
- В остальных случаях в качестве значения для параметра **remote-ip** должен быть указан IP-адрес удаленного узла VPN.
- В том случае если удаленный узел имеет динамический IP-адрес значение для параметра **remote-ip** не указывается, при этом с помощью команды **vpn ipsec site-to-site peer** <*туннель*> **authentication** должны быть указаны идентификационные данные удаленного узла (см. стр.76).

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания IP-адреса удаленного шлюза. В том случае если удаленный узел VPN имеет динамический IP-адрес, параметр remote-ip не используется, при этом должны быть настроены идентификационные данные удаленного узла при помощи команды **vpn ipsec site-to-site peer** <*туннель*> **authentication.**

Форма **set** данной команды используется для указания IP-адреса удаленного шлюза VPN.

Форма **delete** данной команды используется для удаления настройки IP-адреса удаленного шлюза VPN.

Форма **show** данной команды используется для отображения настройки IP-адреса удаленного шлюза VPN.

4.5.8. vpn ipsec site-to-site peer <туннель> local-subnet <ipv4-сеть>

Указание локальной подсети, к которой удаленный шлюз VPN будет иметь доступ.

Синтаксис

```
set vpn ipsec site-to-site peer <туннель> local-subnet <ipv4-сеть>
delete vpn ipsec site-to-site peer <туннель> local-subnet
show vpn ipsec site-to-site peer <туннель> local-subnet
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      site-to-site {
         peer туннель {
            local-subnet ipv4-сеть
         }
      }
   }
}
```

Параметры

туннель

Обязательный. Название туннеля к удаленному узлу IPSec.

ipv4-сеть

Обязательный. IP-адрес локальной сети, расположенной за локальным шлюзом VPN, к которой будет иметь доступ удаленный шлюз VPN. Используемый формат: *ip-адрес/префикс*. Адрес сети 0.0.0.0/0 означает любую сеть.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания IP-адреса локальной подсети, к которой будет иметь доступ удаленный шлюз VPN.

Форма **set** данной команды используется для указания IP-адреса локальной подсети.

Форма **delete** данной команды используется для удаления настройки IP-адреса локальной подсети.

Форма **show** данной команды используется для отображения настройки IP-адреса локальной подсети.

4.5.9. vpn ipsec site-to-site peer <туннель> remote-subnet <ipv4-сеть>

Указание удаленной подсети, расположенной за удаленным шлюзом VPN, к которой будет иметь доступ локальная система Numa Edge.

Синтаксис

```
set vpn ipsec site-to-site peer <туннель> remote-subnet <ipv4-сеть>
delete vpn ipsec site-to-site peer <туннель> remote-subnet
show vpn ipsec site-to-site peer <туннель> remote-subnet
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      site-to-site {
         peer туннель {
            remote-subnet ipv4-сеть
         }
      }
   }
}
```

Параметры

туннель

Обязательный. Название туннеля к удаленному узлу IPSec.

ipv4-сеть

Обязательный. IP-адрес удаленной подсети, расположенной за удаленным шлюзом VPN, к которой будет иметь доступ локальный шлюз VPN. Используемый формат: *ip-адрес/префикс*. Адрес сети 0.0.0.0/0 означает любую сеть.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания IP-адреса удаленной подсети, расположенной за удаленным шлюзом VPN, к которой будет иметь доступ локальный шлюз VPN.

Форма **set** данной команды используется для указания IP-адреса удаленной подсети.

Форма **delete** данной команды используется для удаления настройки IP-адреса удаленной подсети.

Форма **show** данной команды используется для отображения настройки IP-адреса удаленной подсети.

4.5.10. vpn ipsec site-to-site peer <туннель> nat-traversal <состояние>

Определение использования локальным шлюзом VPN технологии NAT-T.

Синтаксис

```
set vpn ipsec site-to-site peer <туннель> nat-traversal <состояние>
delete vpn ipsec site-to-site peer <туннель> nat-traversal
show vpn ipsec site-to-site peer <туннель> nat-traversal
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
   ipsec {
      site-to-site {
         peer туннель {
            nat-traversal состояние
         }
      }
   }
}
```

Параметры

туннель

Обязательный. Название туннеля к удаленному узлу IPSec.

состояние

Включение/отключение NAT-T (RFC 3947). Поддерживаются следующие значения:

- **on**: Включение функциональности NAT-T, в том случае если между узлами будет обнаружен шлюз, обеспечивающий преобразование сетевых адресов.
- **off**: Отключение функциональности NAT-T.
- **force**: Включение функциональности NAT-T, вне зависимости от того, будет ли между узлами обнаружен шлюз, обеспечивающий преобразование сетевых адресов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать системе Numa Edge предлагать использование NAT-T (RFC 3947) при согласовании IKE.

Форма **set** данной команды позволяет указать, следует ли предлагать использование механизма NAT-T при согласовании IKE.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** данной команды используется для отображения настройки.

4.6. Эксплуатационные команды

4.6.1. clear vpn ipsec-peer <туннель>

Перезапуск туннеля к указанному узлу IPSec.

Синтаксис

```
clear vpn ipsec-peer <туннель>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

туннель

Название туннеля к узлу IPSec, который требуется перезапустить.

Указания по использованию

Данная команда используется для перезапуска туннеля IPSec. Перезапуск туннеля IPSec приведет к тому, что туннель будет закрыт и установлен заново.

В том случае если не указан адрес удаленного узла (**remote-ip**) (в том случае если удаленный узел имеет динамический адрес), туннель будет закрыт, но новое подключение не будет инициировано.

4.6.2. clear vpn ipsec-process

Перезапуск процесса IPSec.

Синтаксис

```
clear vpn ipsec-process
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Указания по использованию

Данная команда используется для перезапуска процесса IPSec. Перезапуск IPSec приведет к тому, что все туннели будут закрыты и установлены заново.

4.6.3. show vpn ike rsa-keys

Отображение ключей RSA, о которых есть запись в системе.

Синтаксис

```
show vpn ike rsa-keys
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Указания по использованию

Данная команда используется для отображения всех открытых ключей RSA, о которых есть записи в системе. То есть, при выполнении этой команды, будет выведен открытый ключ локальной системы, а также указанные открытые ключи других узлов VPN.

Примеры

В примере ниже приведен вывод для команды **show vpn ike rsa-keys**, в котором отображены открытые ключи, о которых есть записи на узле V1:

- выведен открытый ключ локальной системы, при этом секретный ключ локальной системы не выводится;
- выведен открытый ключ узла V2.

Пример 1 – "show vpn ike rsa-keys"

```
admin@V1:~$ show vpn ike rsa-keys
```

```
Local public
key0sAQNfpZicOXWl1rMvNWLIfFppq1uWtUvj8esyjBl/zBfrK4ecZbt7WzMdMLiLugYtVgo+zJQV
5dmQnN+n3qkU9ZLM5QWBxG4iLFtYcwC5fCMx0hBJfnIEd68d11h7Ea6J4IAm3ZWXcBeOV4S8mC4HV
+mqZfv3xyh1ELjfmLM3fWkp8g5mX7ymgcTpneHiSYX1T9NU3i2CHjYfeKPFb4zJIopu2R654kODGO
a+4r241Zx3cDIJgHBYSYOiSFYbcdQhKQS3cclFPGVMHYGXjjoiUSA7d2eMabDtIU4FwnqH3qVN/kd
edK34sEJiMUgieT6pJQ6W8y+5PgESvouykx8cyTiOobnx0G9oqFcxYLknQ3GbrPej
========================================================== Peer IP:
10.1.0.55 (V2)
0sAQOVBIJL+rIkpTuwh8FPeceAF0bhgLr++W51bOAIjFbRDbR8gX3Vlz6wiUbMgGwQxWlYQiqsCea
cicsfZx/amlEn9PkSE4e7tqK/JQo40L5C7gcNM24mup1d+0WmN3zLb9Qhmq5q3pNJxEwnVbPPQeId
ZMJxnb1+lA8DPC3SIxJM/3at1/KrwqCAhX3QNFY/zNmOtFogELCeyl4+d54wQljA+3dwFAQ4bboJ7
YIDs+rqORxWd3l3I7IajT/pLrwr5eZ8OA9NtAedbMiCwxyuyUbznxXZ8Z/MAi3xjL1pjYyWjNNiOi
j82QJfMOrjoXVCfcPn96ZN+Jqk+KknoVeNDwzpoahFOseJREeXzkw3/lkMN9N1
admin@V1:~$
```

4.6.4. show vpn ike sa

Вывод сведений обо всех активных в данный момент защищенных соединениях IKE (ISAKMP).

Синтаксис

```
show vpn ike sa [peer <туннель>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

туннель

Название туннеля к узлу IPSec, для которого требуется вывести сведения IKE SA.

Для каждого узла будет существовать максимум одно защищенное соединение IKE SA (за исключением случая с согласованием нового ключа).

Указания по использованию

Данная команда используется для вывода сведений о защищенных соединениях IKE (SA).

Данная команда выводит список узлов VPN и текущее состояние IKE. Выводятся следующие сведения:

- IP-адреса, используемые для IPSec на локальном и удаленном шлюзах VPN.
- Состояние подключения.
- Алгоритм шифрования.
- Алгоритм хеширования.
- Количество времени, в течение которого подключение активно.
- Установленное время жизни для защищенного соединения (SA).
- Используется ли NAT-T (RFC 3947 NAT Traversal).

Примеры

В примере ниже приведен вывод команды **show vpn ike sa**.

Пример 2 – "show vpn ike sa"

```
admin@V1:~$ show vpn ike sa
Source Destination Cookies ST S V E Created Phase2
192.0.2.33:500 192.0.2.1:500 0ace446788cea1d1:8b0f4e5d4b93b633 9 I 10 M 2020-
03-19 12:50:53 3
admin@V1:~$
```

4.6.5. show vpn ike secrets

Вывод настроенных предварительных ключей.

Синтаксис

```
show vpn ike secrets
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Указания по использованию

Данная команда используется для вывода настроенных в системе предварительных ключей. Выводится следующие сведения:

- Локальный IP-адрес
- IP-адрес узла.
- Предварительный ключ.

Примеры

В примере ниже приведен вывод команды **show vpn ike secrets**.

Пример 3 – "show vpn ike secrets"

```
admin@V1:~$ show vpn ike secrets
Local IP Peer IP Secret
101.102.103.104 201.202.203.204 vpn_key_1
101.102.103.104 110.111.112.113 vpn_key_2
```

4.6.6. show vpn ipsec sa

Вывод сведений обо всех активных в данный момент защищенных соединениях IPSec.

Синтаксис

```
show vpn ipsec sa [peer <туннель>]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

туннель

Вывод всех защищенных соединений IPSec SA, ассоциированных с указанным туннелем к узлу IPSec.

Указания по использованию

Данная команда используется для отображения сведений об удаленном узле VPN и активных защищенных соединениях IPSec (SA).

Выводятся следующие сведения:

- IP-адрес удаленного шлюза VPN.
- Направление SA.
- SPI подключения.
- Алгоритм шифрования.
- Алгоритм хеширования.
- Установленное время жизни для защищенного соединения (SA).

Примеры

В примере ниже приведен вывод для команды **show vpn ipsec sa**.

Пример 4 – "show vpn ipsec sa"

```
admin@V1:~$ show vpn ipsec sa
192.0.2.33 192.0.2.1
```

```
esp mode=tunnel spi=216613311(0x0ce941bf) reqid=0(0x00000000)
E: 3des-cbc 34af68cb af4a7204 8adc7ff1 795f77fa b99e4d29 c8ddbdc6
A: hmac-sha1 95038eef cd47219c bf888f9a 0b636bd6 2eddee1c
seq=0x00000000 replay=4 flags=0x00000000 state=mature
created: Mar 19 13:14:55 2020 current: Mar 19 13:32:12 2020
diff: 1037(s) hard: 1800(s) soft: 1440(s)
last: Nov 19 13:16:55 2010 hard: 0(s) soft: 0(s)
current: 240(bytes) hard: 0(bytes) soft: 0(bytes)
allocated: 4 hard: 0 soft: 0
sadb_seq=1 pid=2104 refcnt=0
192.0.2.1 192.0.2.33
esp mode=tunnel spi=209596172(0x0c7e2f0c) reqid=0(0x00000000)
E: 3des-cbc 4e7f89c0 f4a5126b c28949ff 726de9ac 0f055d6c bec8dfec
A: hmac-sha1 7930104c d9771709 227d6c7b 294aaac5 35885a2e
seq=0x00000000 replay=4 flags=0x00000000 state=mature
created: Mar 19 13:14:55 2020 current: Mar 19 13:32:12 2020
diff: 1037(s) hard: 1800(s) soft: 1440(s)
last: Nov 19 13:16:55 2010 hard: 0(s) soft: 0(s)
current: 240(bytes) hard: 0(bytes) soft: 0(bytes)
allocated: 4 hard: 0 soft: 0
sadb_seq=0 pid=2104 refcnt=0
```

4.6.7. show vpn ipsec status

Вывод сведений о состоянии процессов IPSec.

Синтаксис

```
show vpn ipsec status
```

Режим интерфейса

Эксплуатационный режим.

Параметры

Отсутствуют.

Указания по использованию

Данная команда используется для отображения сведений о состоянии процессов IPSec. Также выводится количество активных туннелей.

Примеры

В примере ниже приведен вывод для команды **show vpn ipsec status**.

Пример 5 – "show vpn ipsec status"

```
admin@V1:~$ show vpn ipsec status
IPSec running
4 active tunnels.
admin@V1:~$
```

4.7. Управление RSA ключами

4.7.1. vpn rsa-keys delete <имя_ключа>

Удаление ключевой пары RSA из системного хранилища.

Синтаксис

```
vpn rsa-keys delete имя_ключа
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_ключа

Обязательный. Имя ключевой пары RSA, который будет удален.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для удаления файла, содержащего ключевую пару RSA. Данная команда доступна только для пользователей, обладающих правами администратора. Удалять ключи, используемые в конфигурации, запрещено.

4.7.2. vpn rsa-keys export <имя_ключа> to <имя_файла>

Экспорт открытого ключа из ключевой пары, используемого на другом устройстве для установки соединения.

Синтаксис

```
vpn rsa-keys export имя_ключа to <имя_файла>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_ключа

Обязательный. Имя ключевой пары RSA, которая находится в системном хранилище ключей.

имя_файла

Обязательный. Имя локального или удалённого файла. Задает имя для открытого ключа RSA, который будет создан после экспорта из системного хранилища ключей. Допустимые значения:

- **<filename>** - имя локального или удаленного файла;
- **<ftp://user@host/file>** - имя локального или удаленного файла;
- **<scp://user@host/file>** - имя локального или удаленного файла;
- **<tftp://host/file>** - имя локального или удаленного файла.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для экспорта файла, содержащего открытый ключ RSA, и который используется при применении механизма безопасности с использованием ассиметричной криптографии. Данная команда доступна только для пользователей, обладающих правами администратора.

4.7.3. vpn rsa-keys generate <имя_ключа> bits <размер>

Генерация файла, содержащего ключевую пару RSA.

Синтаксис

```
vpn rsa-keys generate имя_ключа
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_файла

Обязательный. Имя ключевой пары RSA, которая будет создана.

размер

Указание размера генерируемых ключей в битах. Доступный диапазон <1024-16384>. Значение по умолчанию 2192.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для создания файла, содержащего ключевую пару RSA, и который используется при применении механизма безопасности с использованием ассиметричной криптографии. После выполнения данной команды создается файл, содержащий открытый и закрытый RSA ключи указанного размера. Данный файл хранится в системном хранилище ключей, в каталоге **/var/lib/edge/ipsec/.** Данная команда доступна только для пользователей, обладающих правами администратора.

4.7.4. vpn rsa-keys import <имя_ключа> from <имя_файла>

Импорт открытого ключа RSA в системное хранилище.

Синтаксис

```
vpn rsa-keys import имя_ключа from <имя_файла>
```

Режим интерфейса

Эксплуатационный режим.

Параметры

имя_ключа

Обязательный. Имя открытого ключа RSA, который будет импортирован.

имя_файла

Обязательный. Имя локального или удалённого файла. Задает расположение открытого ключа RSA, который будет импортирован в системное хранилище ключей. Допустимые значения:

- **<filename>** - имя локального или удаленного файла;
- **<ftp://user@host/file>** - имя локального или удаленного файла;
- **<scp://user@host/file>** - имя локального или удаленного файла;
- **<tftp://host/file>** - имя локального или удаленного файла.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для импорта файла, содержащего открытый RSA ключ, и который используется при применении механизма безопасности с использованием ассиметричной криптографии. Данная команда доступна только для пользователей, обладающих правами администратора.

4.7.5. vpn rsa-keys list

Просмотр файлов RSA ключей в системном хранилище.

Синтаксис

```
vpn rsa-keys list
```

Режим интерфейса

Эксплуатационный режим.

Параметры

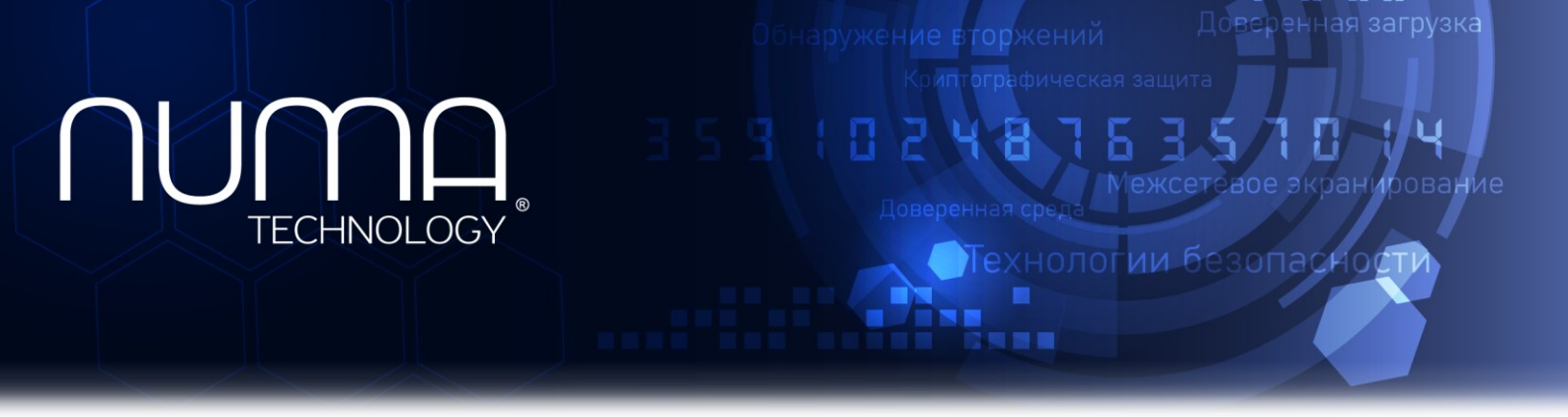
Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для просмотра RSA ключей, находящихся в системном хранилище.



Межсетевой экран Numa Edge

Руководство администратора

Туннелирование IP

Листов 23

Санкт-Петербург
2022

СОДЕРЖАНИЕ

ИДЕНТИФИКАЦИЯ ДОКУМЕНТА

Название документа	Руководство администратора. Туннелирование IP
Версия документа	1.1
Обозначение документа	643.АМБН.00004-01 32 07
Идентификация ОО	Межсетевой экран Numa Edge
Идентификация разработчика	ООО «НумаТех»
Ключевые слова	Межсетевой экран, МЭ, tunnel

1. ТУННЕЛИРОВАНИЕ IP

1.1. Обзор технологий туннелирования

Туннелирование IP - это механизм для инкапсуляции пакетов одного сетевого протокола в пакеты другого протокола. Пакеты инкапсулируемого протокола («пассажирский» протокол) вкладываются в пакеты транспортного протокола (протокола «носителя»). Инкапсулированный пакет перенаправляется в сеть назначения, затем извлекается вложенный пакет, который перенаправляется получателю.

В системе Numa Edge поддерживаются три наиболее часто используемых механизма туннелирования:

- туннели на основе протокола GRE (Generic Routing Encapsulation) могут быть использованы для транспортировки отличных от IP-протоколов таких как Novell IPX, Banyan VINES, AppleTalk и DECNet. Они также могут использоваться для переноса многоадресных и широковещательных передач, а также трафика протокола IPv6. Для того, чтобы иметь возможность включать туннельные интерфейсы GRE в состав мостовых групп, необходимо создать туннель GRE специального типа. Для этого используется параметр **gre-bridge** команды **interfaces tunnel <tunx> encapsulation**;
- туннели IP-IP могут быть использованы только для переноса трафика протокола IPv4;
- туннели SIT (Simple Internet Transition) могут быть использованы для транспортировки пакетов протокола IPv6 через сеть с транспортной технологией, поддерживающей только маршрутизацию IPv4.

Логические интерфейсы, которые отправляют пакеты IP в туннельном режиме, называются туннельными интерфейсами.

Туннельные интерфейсы ведут себя точно так же, как любые другие интерфейсы, настроенные в системе: на их основе можно настраивать маршрутизацию, межсетевое экранирование, NAT, а также другие возможности, предоставляемые системой для работы с интерфейсами. Управлять туннельными интерфейсами можно с использованием стандартных команд.

Следует помнить, что туннели GRE, IP-IP и SIT не обеспечивают безопасности передаваемых данных.

1.2. Туннели GRE

Протокол GRE обеспечивает простой универсальный механизм инкапсуляции пакетов различных сетевых протоколов для их переноса другим протоколом. Исходный пакет («пассажирский» пакет) может относиться к одному из произвольных сетевых протоколов — например, это может быть многоадресный пакет, пакет IPv6 или пакет одного из отличных от IP LAN протоколов таких как AppleTalk, Banyan VINES или Novell IPX. В качестве транспортного протокола может быть использован один из маршрутизируемых IP-протоколов. Пакет пассажирского протокола первоначально инкапсулируется в пакет GRE, таким образом создается «туннель» GRE. Затем пакет GRE инкапсулируется в пакет транспортного протокола (протокола «носителя»), который затем перенаправляется в сеть назначения, после чего извлекается исходный пакет и доставляется адресату.

Протокол GRE может быть использован в следующих целях:

- объединение сетей на базе не-IP-протоколов через глобальную сеть IP. Трафик отличных от IP-протоколов, таких как Novell IPX или Appletalk не может быть маршрутизован через сеть IP. Туннель GRE позволяет создать виртуальный канал типа «точка-точка» между двумя такими локальными сетями через ГВС;
- маршрутизация пакетов IPv6 через сеть IPv4;

- шифрование трафика при использовании многоадресной передачи. IPSec, который является стандартным механизмом для обеспечения безопасности в сетях IP, не может быть использован для шифрования трафика при многоадресной передаче. Однако многоадресные пакеты можно инкапсулировать в туннель GRE и затем маршрутизировать через соединение VPN, таким образом инкапсулированные пакеты будут защищены при помощи IPSec.

Туннели GRE не имеют контроля состояния, то есть протокол не имеет средств для автоматического отслеживания состояния или доступности оконечных узлов. Однако существует возможность отслеживать состояние другого оконечного узла, отправляя ему специальные сообщения, подтверждающие активность. Другое оконечное устройство считается неактивным, если оно перестает отвечать на данные сообщения.

GRE не имеет средств для обеспечения безопасности. Существует возможность настроить ключ на каждом из оконечных узлов туннеля, который позволяет оконечным точкам аутентифицировать друг друга. Но следует учитывать, что данный ключ передается в каждом пакете в открытом виде. В том случае если требуется обеспечить безопасность передаваемых данных, GRE может быть использован совместно с IPSec. GRE использует номер протокола IP 47.

1.3. Туннели GRE, которые могут быть включены в состав мостовой группы

Одним из ограничений обычных туннелей GRE является то, что их нельзя включать в состав мостовых групп. Для того чтобы иметь возможность включения туннельных интерфейсов GRE в состав сетевого моста, необходимо создать туннель GRE специального типа, для этого используется параметр **gre-bridge** команды **interfaces tunnel <tunx> encapsulation**. Туннели такого типа должны быть использованы только в тех случаях, когда туннельные интерфейсы требуется включить в состав мостовой группы. Более подробная информация о настройке мостовых групп приведена в разделе «Настройка мостов» документа «Руководство администратора».

1.4. Туннели IP-IP

Протокол инкапсуляции IP-IP определяет механизм, позволяющий вкладывать (инкапсулировать) пакет IP в другой пакет IP, используемый для транспортировки. Например, туннель IP-IP может быть использован для обеспечения прохождения пакетов многоадресной передачи через участок сети (например, туннель IPSec), который не поддерживает многоадресную маршрутизацию. Также туннель IP-IP может быть использован для того, чтобы повлиять на маршрутизацию пакета, или для доставки пакета на мобильное устройство с использованием Mobile IP.

При инкапсуляции IP-IP второй заголовок IP вставляется перед заголовком IP исходного пакета (пакета «пассажира»). В новом заголовке IP в качестве адресов отправителя и получателя указываются адреса оконечных точек туннеля. В заголовке IP исходного пакета указаны первоначальные отправитель и получатель. После того как инкапсулированный пакет приходит в оконечную точку туннеля, внутренний заголовок IP извлекается, и исходный пакет IP доставляется конечному получателю.

Механизм инкапсуляции IP-IP прост и надежен. Однако он имеет ряд ограничений:

- при использовании туннелирования IP-IP не может быть инкапсулирован широковещательный трафик;
- при использовании туннелирования IP-IP не может быть инкапсулирован трафик IPv6. Для доставки трафика такого вида может быть использовано туннелирование на базе GRE.

Так же, как и GRE, туннелирование IP-IP не имеет средств для обеспечения безопасности передаваемых данных. В том случае если это необходимо, туннелирование IP-IP может быть использовано совместно с IPSec.

1.5. Протокол SIT

Набор протоколов SIT (Simple Internet Transition) был разработан для обеспечения взаимодействия узлов IPv4 и узлов IPv6.

Одним из механизмов, обеспечиваемых SIT, является механизм инкапсуляции пакетов IPv6 в пакеты IPv4 для транспортировки их через те сегменты сети, которые поддерживают только маршрутизацию на базе IPv4.

Для создания туннеля SIT используется параметр **sit** команды **interfaces tunnel <tunx> encapsulation**.

1.6. Туннельные интерфейсы и IPSec

GRE, IP-IP и SIT туннели не шифруются и не обеспечивают никакой защиты помимо использования паролей, которые в свою очередь передаются открытым текстом в каждом пакете. Это означает, что GRE, IP-IP и SIT туннели сами по себе не обеспечивают адекватной защиты передаваемой информации.

В то же время, туннели IPSec не могут напрямую маршрутизировать трафик протоколов, отличных от IP или широковещательные протоколы. IPSec также имеет ряд ограничений с эксплуатационной точки зрения. Использование туннельных интерфейсов в сочетании с IPSec VPN позволяет обеспечить безопасные, маршрутизируемые подключения между шлюзами, которые имеют некоторые преимущества по сравнению с использованием туннелей на основе IPSec:

- поддержка стандартных эксплуатационных команд, например, **show interfaces**;
- поддержка таких средств, как traceroute и SNMP;
- динамическое переключение на другой туннель в случае отказа;
- упрощенные политики IPSec и выявление неисправностей.

Для создания безопасных маршрутизируемых туннелей необходимо использовать туннели GRE, IP-IP и SIT совместно с подключением IPSec, таким образом, чтобы туннель IP был защищен при помощи туннеля IPSec. Пример настройки туннеля IPSec для обеспечения защиты туннеля GRE приведен в разделе «Защита туннеля GRE с использованием IPSec».

Примечание. Механизм IPSec доступен только в исполнении Numa Edge VPN.

1.7. Туннельные интерфейсы и QoS

В процессе маркировки трафика происходит кодирование трех старших битов поля ToS. Для туннелей сетевого уровня (туннелей типов GRE, IP-IP и SIT) производится копирование поля ToS из внутреннего во внешний пакет. Копирование поля ToS для туннелей канального уровня не осуществляется.

Для внешнего пакета также предусмотрена возможность принудительного указания значения 6 бит поля DSCP (Differencial Service Code Point) с помощью команды **interfaces tunnel <tunx> dscp <значение>**.

1.8. Настройка туннелирования

В данном разделе приведены примеры настройки туннелей GRE.

В данном разделе рассматриваются следующие вопросы:

- Перед началом настройки.
- Настройка базового туннеля GRE.
- Настройка дополнительных параметров туннеля GRE.
- Объединение туннелей GRE в сетевой мост.

1.8.1. Перед началом настройки

В этом наборе примеров предполагается использование двух систем Numa Edge с именами узлов edge1 и edge2.

Все интерфейсы Ethernet, используемые в настройке туннеля, должны быть заранее настроены. В этом примере используется интерфейс eth1 на узле edge1 и интерфейс eth1 на узле edge2.

1.8.2. Настройка базового туннеля GRE

В данном разделе приведены примеры настройки базового туннеля GRE между системами Numa Edge с именами edge1 и edge2. Сначала настраивается узел edge1, затем узел edge2.

Для базового туннеля защита при помощи пароля не осуществляется: это значит, что он не обеспечивает безопасность передаваемых данных и не рекомендован к использованию в производственных условиях. После завершения настройки узлы будут настроены в соответствии с рисунком 1.

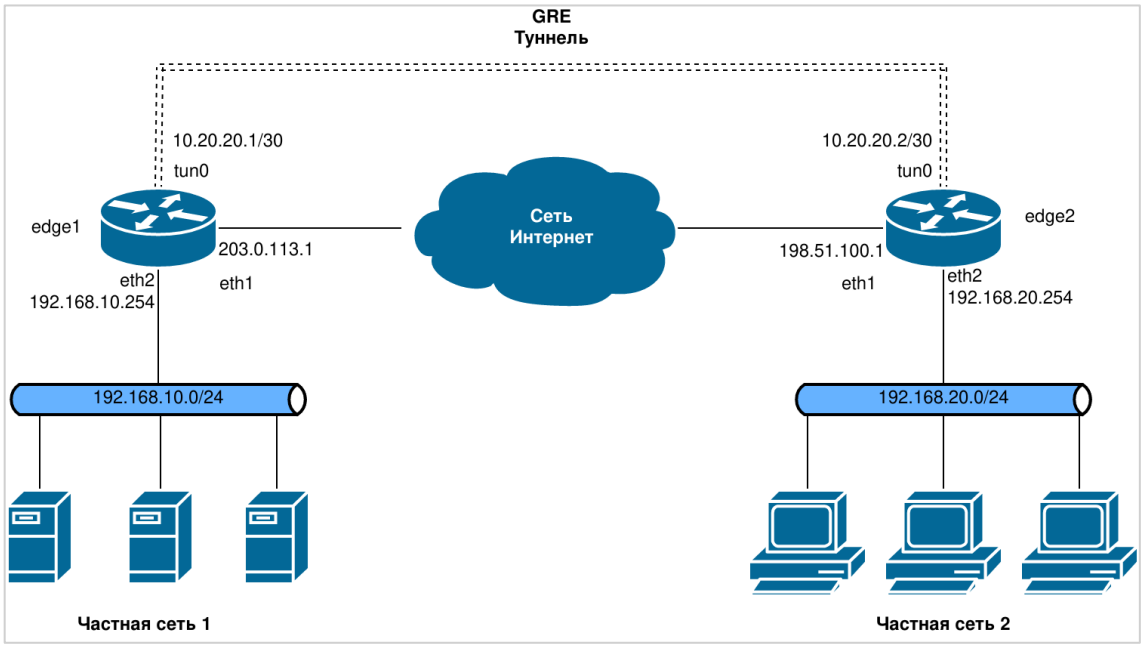


Рисунок 1 – Настройка базового туннеля GRE

1.8.2.1. Настройка узла edge1

В примере 1 настраивается туннель GRE от узла edge1 к узлу edge2 через ГВС. В данном примере приведено создание туннельного интерфейса и оконечной точки туннеля на узле edge1:

- туннельному интерфейсу tun0 на узле edge1 назначается IP-адрес 10.20.20.1 из сети 10.20.20.0/30;
- в качестве адреса локальной оконечной точки туннеля (**local-ip**) в этом примере используется адрес 203.0.113.1, назначенный интерфейсу **eth1**;
- в качестве IP-адреса удаленного оконечного узла туннеля (**remote-ip**) используется адрес 198.51.100.1 на узле edge2.

В примере 1 приведено создание туннельного интерфейса и оконечного узла туннеля на узле edge1. Для этого необходимо выполнить следующие действия на узле edge1 в режиме настройки.

Пример 1 – Создание оконечного узла базового туннеля GRE на узле edge1

Действие	**Команда**
Создание туннельного интерфейса и назначение ему IP-адреса.	`[edit]` `admin@edge1# set interfaces tunnel tun0 address 10.20.20.1/30`
Указание IP-адреса источника для данного туннеля.	`[edit]` `admin@edge1# set interfaces tunnel tun0 local-ip 203.0.113.1`
Указание IP-адреса удаленного оконечного узла туннеля.	`[edit]` `admin@edge1# set interfaces tunnel tun0 remote-ip 198.51.100.1`
Указание режима инкапсуляции для туннеля.	`[edit]` `admin@edge1# set interfaces tunnel tun0 encapsulation gre`
Указание краткого текстового описания для туннеля.	`[edit]` `admin@edge1# set interfaces tunnel tun0 description "GRE tunnel to edge2"`
Фиксация настройки.	`[edit]` `admin@edge1# commit`

Вывод настройки.	`[edit]`
	`admin@edge1# show interfaces tunnel tun0`
	`address 10.20.20.1/30`
	`description "Tunnel to edge2"`
	`encapsulation gre`
	`local-ip 203.0.113.1`
	`remote-ip 198.51.100.1`

Добавление статического интерфейсного маршрута к сети 192.168.20.0/24 через туннель.	`[edit]` `admin@edge1# set protocols static interface-route 192.168.20.0/24 next-hop-interface tun0`
Фиксация настройки.	`[edit]` `admin@edge1# commit`

1.8.2.2. Настройка узла edge2

В этом разделе приведена настройка оконечного узла туннеля на узле edge2:

- туннельному интерфейсу tun0 на узле edge2 назначается IP-адрес 10.20.20.2 из сети 10.20.20.0/30;
- в качестве адреса источника для оконечной точки туннеля (**local-ip**) в этом примере используется адрес 198.51.100.1;
- в качестве IP-адреса удаленного оконечного узла туннеля (**remote-ip**) используется адрес 203.0.113.1 на узле edge1;
- создается статический маршрут для обеспечения доступа к удаленной локальной сети через созданный туннель.

В примере 2 приведено создание оконечного узла туннеля на узле edge2. Для этого необходимо выполнить следующие действия на узле edge2 в режиме настройки.

Пример 2 – Создание оконечного узла базового туннеля GRE на узле edge2

Действие	**Команда**
Создание туннельного интерфейса и назначение ему IP-адреса.	`[edit]` `admin@edge2# set interfaces tunnel tun0 address 10.20.20.2/30`

Действие	Команда
Указание IP-адреса источника для данного туннеля.	[edit] admin@edge2# set interfaces tunnel tun0 local-ip 198.51.100.1
Указание IP-адреса удаленного оконечного узла туннеля.	[edit] admin@edge2# set interfaces tunnel tun0 remote-ip 203.0.113.1
Указание режима инкапсуляции для туннеля.	[edit] admin@edge2# set interfaces tunnel tun0 encapsulation gre
Указание краткого текстового описания для туннеля.	[edit] admin@edge2# set interfaces tunnel tun0 description "GRE tunnel to edge1"
Фиксация настройки.	[edit] admin@edge2# commit
Вывод настройки.	[edit] admin@edge2# show interfaces tunnel tun0 address 10.20.20.2/30 description "Tunnel to edge1" encapsulation gre local-ip 198.51.100.1 remote-ip 203.0.113.1
Добавление статического интерфейсного маршрута к сети 192.168.40.0/24 через туннель.	[edit] admin@edge2# set protocols static interface-route 192.168.10.0/24 next-hop-interface tun0
Фиксация настройки.	[edit] admin@edge2# commit

1.8.3. Настройка дополнительных параметров туннеля GRE

В данном разделе приведены дополнительные параметры настройки для туннельных интерфейсов, определенных в предыдущем примере:

- настраиваются ключи, позволяющие оконечным точкам аутентифицировать друг друга. Эти ключи должны совпадать на обоих оконечных узлах;
- для каждого оконечного узла указываются значения TTL, DSCP и MTU;
- к каждому туннельному интерфейсу применяется политика межсетевого экранирования.

1.8.3.1. Настройка узла edge1

В примере 3 приведены дополнительные параметры настройки для оконечного узла edge1, созданного в примере 1:

- значение TTL для пакетов устанавливается равным 220, значение поля DSCP устанавливается равным 55, а значение MTU для пакетов устанавливается равным 1460;
- к туннельному интерфейсу применяется две политики межсетевого экранирования:
  - набор tun0-fw-in применяется к пакетам, входящим через туннельный интерфейс;
  - набор правил tun0-fw-out применяется к пакетам, покидающим туннельный интерфейс.

В данном примере предполагается, что эти наборы правил заранее определены.

Так как настройку ключа аутентификации можно указать только при создании туннеля, в примере 3 предполагается создание нового туннеля с параметрами из примера 1, ниже приведены только отличающиеся параметры.

Для настройки оконечной точки туннеля GRE, необходимо выполнить следующие шаги на узле edge1 в режиме настройки.

Пример 3 – Добавление значений в настройку оконечного узла туннеля GRE на узле edge1

Действие	**Команда**
Установка TTL.	[edit] admin@edge1# set interfaces tunnel tun0 ttl 220
Установка DSCP.	[edit] admin@edge1# set interfaces tunnel tun0 dscp 55
Установка MTU.	[edit] admin@edge1# set interfaces tunnel tun0 mtu 1460
Применение правил межсетевого экрана к входящим пакетам.	[edit] admin@edge1# set interfaces tunnel tun0 policy in firewall tun0-fw-in
Применение правил межсетевого экрана к исходящим пакетам.	[edit] admin@edge1# set interfaces tunnel tun0 policy out firewall tun0-fw-out
Фиксация настройки.	[edit] admin@edge1# commit

Вывод настройки.	[edit]
	admin@edge1# show interfaces tunnel tun0
	address 10.20.20.1/30
	description “Tunnel to edge2”
	dscp 55
	encapsulation gre
	firewall {
	in {
	name tun0-fw-in
	}
	out {
	name tun0-fw-out
	}
	}
	local-ip 203.0.113.1
	remote-ip 198.51.100.1
	mtu 1460
	ttl 220

1.8.3.2. Настройка узла edge2

В примере 4 приведены дополнительные параметры настройки для оконечного узла туннеля в системе edge2, созданного в примере 2:

- значение TTL установлено равным 220, значение поля DSCP установлено равным 55, а значение MTU установлено равным 1460;
- к туннельному интерфейсу применяются две политики межсетевого экранирования:
  - набор правил tun0-fw-in применяется к пакетам, входящим на туннельный интерфейс;
  - набор правил tun0-fw-out применяется к пакетам, покидающим туннельный интерфейс.

В данном примере предполагается, что эти наборы правил заранее определены.

Так как настройку ключа аутентификации можно указать только при создании туннеля, в примере 4 предполагается создание нового туннеля с параметрами из примера 2, ниже приведены только отличающиеся параметры.

Для этого необходимо выполнить следующие действия на узле edge2 в режиме настройки.

Пример 4 – Добавление значений в настройку оконечного узла туннеля GRE на узле edge2

Действие	**Команда**
Установка TTL.	`[edit]` `admin@edge2# set interfaces tunnel tun0 ttl 220`
Установка DSCP.	`[edit]` `admin@edge2# set interfaces tunnel tun0 dscp 55`
Установка MTU.	`[edit]` `admin@edge2# set interfaces tunnel tun0 mtu 1460`
Применение правил межсетевого экрана к входящим пакетам.	`[edit]` `admin@edge2# set interfaces tunnel tun0 policy in firewall tun0-fw-in`
Применение правил межсетевого экрана к исходящим пакетам.	`[edit]` `admin@edge2#  set interfaces tunnel tun0 policy out firewall tun0-fw-out`
Фиксация настройки.	`[edit]` `admin@edge2# commit`

Вывод настройки.	`[edit]`
	`admin@edge2# show interfaces tunnel tun0`
	`address 10.20.20.2/30`
	`description “Tunnel to edge1”`
	`dscp 55`
	`encapsulation gre`
	`firewall {`
	`in {`
	`name tun0-fw-in`
	`}`
	`out {`
	`name tun0-fw-out`
	`}`
	`}`
	`key 101088`
	`local-ip 198.51.100.1`
	`mtu 1460`
	`remote-ip 203.0.113.1`
	`ttl 220`

1.9. Объединение туннелей GRE в сетевой мост

Для того чтобы включить туннельный интерфейс в состав сетевого моста, необходимо создать туннель GRE специального типа. Для этого используется параметр **gre-bridge** команды **interfaces tunnel <tunx> bridge-group bridge <идентификатор_группы>**. Туннели такого типа должны быть использованы только в тех случаях, когда туннельные интерфейсы требуется включить в состав мостовой группы. Более подробная информация о настройке мостовых групп приведена в разделе «Настройка мостов» документа «Руководство администратора» 643.АМБн.00004-01 32 07.

2. КОМАНДЫ ТУННЕЛИРОВАНИЯ

Таблица 1 – Команды настройки туннелирования

Команды режима настройки	
interfaces tunnel <tunx>	Определение туннельного интерфейса.
interfaces tunnel <tunx> address <ipv4-адрес>	Установка первичного или вторичного IP-адреса для туннельного интерфейса.
interfaces tunnel <tunx> description <описание>	Указание краткого текстового описания для туннельного интерфейса.
interfaces tunnel <tunx> disable	Отключение туннельного интерфейса с сохранением текущей настройки.
interfaces tunnel <tunx> dscp <значение>	Указание значения, которое будет записано в поле DSCP (Differentiated Services Code Point) заголовка транспортного пакета IP.
interfaces tunnel <tunx> encapsulation	Установка используемого типа инкапсуляции пакетов.
interfaces tunnel <tunx> key <ключ>	Указание ключа аутентификации для туннельного интерфейса.
interfaces tunnel <tunx> local-ip <ipv4-адрес>	Указание IP-адреса локального оконечного узла туннеля.
interfaces tunnel <tunx> mtu <mtu>	Установка размера MTU для данного туннельного интерфейса.
interfaces tunnel <tunx> multicast <режим>	Установка режима передачи пакетов многоадресной рассылки через туннель.
interfaces tunnel <tunx> remote-ip <ipv4-адрес>	Указание IP-адреса удаленного оконечного узла туннеля.
interfaces tunnel <tunx> ttl <значение>	Указание значения TTL, которое будет записано в заголовок транспортного пакета IP.
Команды эксплуатационного режима	
clear interfaces tunnel counters	Очистка статистической информации для туннельных интерфейсов.
show interfaces tunnel	Вывод сведений для туннельных интерфейсов.

2.1. interfaces tunnel <tunx>

Определение туннельного интерфейса.

Синтаксис

```
set interfaces tunnel <tunx>
delete interfaces tunnel <tunx>
show interfaces tunnel <tunx>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    tunnel tun0..tun999 {
    }
}
```

Параметры

tunx

Обязательный. Идентификатор определяемого туннельного интерфейса. Значение должно лежать в диапазоне от tun0 до tun999.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет создать туннельный интерфейс для инкапсуляции сетевого трафика.

Форма **set** данной команды используется для создания туннельного интерфейса.

Форма **delete** данной команды используется для удаления туннельного интерфейса и его настройки.

Форма **show** данной команды используется для отображения настройки туннельного интерфейса.

2.2. interfaces tunnel <tunx> address <ipv4-адрес>

Установка первичного или вторичного IP-адреса для туннельного интерфейса.

Синтаксис

```
set interfaces tunnel <tunx> address <ipv4-адрес>
delete interfaces tunnel <tunx> address <ipv4-адрес>
show interfaces tunnel tunx address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    tunnel tunx {
        address ipv4-адрес
    }
}
```

Параметры

tunx

Обязательный. Множественный узел. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от tun0 до tun999.

ipv4-адрес

Множественный узел. IPv4-адрес в следующем формате*: IP-адрес*/*префикс*. Для того чтобы назначить интерфейсу несколько адресов, следует создать соответствующее количество узлов конфигурации **address**.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет назначить IP-адрес туннельному интерфейсу. По крайней мере один адрес должен быть определен для туннельного интерфейса.

Форма **set** данной команды используется для назначения IP-адреса туннельному интерфейсу. Обратите внимание, что команду **set** нельзя использоваться для изменения существующего адреса; необходимо удалить адрес, который нужно изменить и создать новый.

Форма **delete** данной команды используется для удаления настройки IP-адреса для туннельного интерфейса. При этом должен остаться по крайней мере один настроенный адрес.

Форма **show** данной команды используется для отображения настройки адреса туннельного интерфейса.

2.3. interfaces tunnel <tunx> description <описание>

Указание краткого текстового описания для туннельного интерфейса.

Синтаксис

```
set interfaces tunnel <tunx> description <описание>
delete interfaces tunnel <tunx> description
show interfaces tunnel <tunx> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    tunnel tunx {
        description текст
    }
}
```

Параметры

tunx

Обязательный. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от tun0 до tun999.

описание

Краткое текстовое описание туннельного интерфейса. По умолчанию установлена пустая строка.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет создать краткое текстовое описание для туннельного интерфейса. Строки, содержащие пробелы, должны быть заключены в двойные кавычки.

Форма **set** данной команды используется для создания краткого текстового описания для туннельного интерфейса.

Форма **delete** данной команды используется для удаления настройки краткого текстового описания туннельного интерфейса.

Форма **show** данной команды используется для отображения настройки краткого текстового описания для туннельного интерфейса.

2.4. interfaces tunnel <tunx> disable

Отключение туннельного интерфейса с сохранением текущей настройки.

Синтаксис

```
set interfaces tunnel <tunx> disable
delete interfaces tunnel <tunx> disable
show interfaces tunnel <tunx>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    tunnel tunx {
        disable
    }
```

```
}
```

Параметры

tunx

Обязательный. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от tun0 до tun999.

Значение по умолчанию

По умолчанию туннельный интерфейс включен (используется).

Указания по использованию

Данная команда используется для отключения туннельного интерфейса без удаления настройки.

Форма **set** данной команды используется для отключения туннельного интерфейса.

Форма **delete** данной команды используется для включения туннельного интерфейса.

Форма **show** данной команды используется для отображения настройки туннельного интерфейса.

2.5. interfaces tunnel <tunx> dscp <значение>

Указание значения, которое будет записано в поле DSCP (Differentiated Services Code Point) заголовка транспортного пакета IP.

Синтаксис

```
set interfaces tunnel <tunx> dscp <значение>
delete interfaces tunnel <tunx> dscp
show interfaces tunnel <tunx> dscp
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    tunnel tunx {
        dscp текст
    }
}
```

Параметры

tunx

Обязательный. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от tun0 до tun999.

значение

Необязательный. Значение DSCP, которое будет записано в заголовок транспортного пакета. Значение может быть указано в форме десятичного числа (в диапазоне от 0 до 63) или в форме стандартного имени из файла /etc/iproute2/rt_dsfield (например, **lowdelay**).

Значение по умолчанию

Значение поля DSCP инкапсулированного пакета копируется в поле DSCP заголовка транспортного пакета (пакета «носителя»).

Указания по использованию

Данная команда определяет значение, указываемое в поле DSCP заголовка транспортного пакета IP.

DSCP — поле в пакете IP, позволяющее назначить сетевому трафику различные уровни обслуживания. Для достижения этого каждый пакет в сети помечается кодом DSCP и соответствующим ему уровнем обслуживания.

Форма **set** данной команды используется для указания значения поля DSCP, указываемого в заголовке IP транспортного пакета.

Форма **delete** данной команды используется для восстановления значения, принятого по умолчанию

Форма **show** данной команды используется для отображения настройки значения DSCP.

2.6. interfaces tunnel <tunx> encapsulation

Установка используемого типа инкапсуляции пакетов.

Синтаксис

```
set interfaces tunnel <tunx> encapsulation {gre | gre-bridge | ipip | sit}
delete interfaces tunnel <tunx> encapsulation
show interfaces tunnel <tunx> encapsulation
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    tunnel tunx {
        encapsulation [gre|gre-bridge|ipip|sit]
    }
}
```

Параметры

tunx

Обязательный. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от tun0 до tun999.

gre

Использование протокола GRE (Generic Routing Encapsulation) для инкапсуляции транспортируемых пакетов.

gre-bridge

Использование протокола GRE (Generic Routing Encapsulation) для инкапсуляции транспортируемых пакетов. Туннели GRE, которые могут быть объединены в сетевые мосты, должны быть использованы только в тех случаях, когда туннельные интерфейсы требуется включить в состав мостовой группы.

ipip

Использование IP-IP для инкапсуляции транспортируемых пакетов.

sit

Использование SIT (Simple Internet Transition) для инкапсуляции.

Значение по умолчанию

Используется протокол GRE.

Указания по использованию

Данная команда позволяет указать тип инкапсуляции для данного туннеля.

Протокол GRE обеспечивает простой универсальный механизм для инкапсуляции пакетов различных сетевых протоколов для их переноса другим протоколом. Исходный пакет («пассажирский» пакет) может относиться к одному из произвольных сетевых протоколов — например, это может быть многоадресный пакет, пакет IPv6 или пакет одного из отличных от IP LAN

протоколов, таких как AppleTalk, Banyan VINES или Novell IPX. В качестве транспортного протокола может быть использован один из маршрутизируемых IP-протоколов. Одним из ограничений обычных туннелей GRE является то, что их нельзя включать в состав мостовых групп. Для того чтобы туннельный интерфейс GRE можно было включить состав сетевого моста, необходимо создать туннель GRE специального типа (с использованием ключевого слова **gre-bridge**). Туннели GRE указанного типа должны быть использованы только в тех случаях, когда туннельные интерфейсы требуется включить в состав мостовой группы. Более подробные сведения о настройке сетевых мостов приведены в разделе «Настройка мостов» документа «Руководство администратора».

Туннель IP-IP может быть использован для обеспечения прохождения пакетов многоадресной передачи через участок сети (например, туннель IPSec), который не поддерживает многоадресную маршрутизацию. Также туннель IP-IP может быть использован для доставки пакета на мобильное устройство с использованием Mobile IP.

Туннели SIT (Simple Internet Transition) могут быть использованы для транспортировки пакетов протокола IPv6 через сети, поддерживающие только IPv4-маршрутизацию.

Форма **set** данной команды используется для указания используемого механизма инкапсуляции для туннельного интерфейса.

Форма **delete** данной команды используется для удаления настройки и восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки.

2.7. interfaces tunnel <tunx> key <ключ>

Указание ключа аутентификации для туннельного интерфейса.

Синтаксис

```
set interfaces tunnel <tunx> key <ключ>
delete interfaces tunnel <tunx> key
show interfaces tunnel <tunx> key
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    tunnel tunx {
        key 0-999999
    }
}
```

Параметры

tunx

Обязательный. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от tun0 до tun999.

ключ

Ключ, который используется локальной и удаленной оконечной точкой для аутентификации друг друга. Для того чтобы туннель мог быть установлен, ключ должен совпадать на обеих оконечных точках туннеля.

Значение по умолчанию

Ключ не настроен, аутентификация не используется.

Указания по использованию

Данная команда позволяет включить обязательную аутентификацию оконечных точек туннеля на основе паролей. Для того чтобы туннель мог быть установлен, ключи должны совпадать

на обеих оконечных точках туннеля. Ключ аутентификации можно настроить только для туннелей GRE.

Примечание. Возможность задания ключа присутствует только на этапе создания туннеля. В случае необходимости задания ключа для уже существующего туннеля и/или изменения его значения, необходимо полностью удалить конфигурацию туннельного интерфейса и настроить заново, указав значение ключа.

Форма **set** данной команды используется для указания ключа аутентификации.

Форма **delete** данной команды используется для удаления ключа аутентификации.

Форма **show** данной команды используется для отображения настройки ключа для данного туннельного интерфейса.

2.8. interfaces tunnel <tunx> local-ip <ipv4-адрес>

Указание IP-адреса локального оконечного узла туннеля.

Синтаксис

```
set interfaces tunnel <tunx> local-ip <ipv4-адрес>
delete interfaces tunnel <tunx> local-ip
show interfaces tunnel <tunx> local-ip
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    tunnel tunx {
        local-ip ipv4-адрес
    }
}
```

Параметры

tunx

Обязательный. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от tun0 до tun999.

ipv4-адрес

Обязательный. IPv4-адрес оконечной точки туннеля на локальном маршрутизаторе. IP-адрес должен быть заранее настроен на интерфейсе.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания IP-адреса локальной оконечной точки туннеля.

Форма **set** данной команды используется для указания адреса локальной оконечной точки туннеля.

Фора **delete** данной команды используется для удаления настройки локальной оконечной точки туннеля. Для обеспечения работы туннеля необходимо настроить обе оконечные точки туннеля.

Форма **show** данной команды используется для отображения настройки локальной оконечной точки туннеля.

2.9. interfaces tunnel <tunx> mtu <mtu>

Установка размера MTU для данного туннельного интерфейса.

Синтаксис

```
set interfaces tunnel <tunx> mtu <mtu>
delete interfaces tunnel <tunx> mtu
show interfaces tunnel <tunx> mtu
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    tunnel tunx {
        mtu 64-8024
    }
}
```

Параметры

tunx

Обязательный. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от tun0 до tun999.

mtu

Необязательный. Размер MTU, в октетах, для данного туннельного интерфейса. Значение должно лежать в диапазоне от 64 до 8024.

Значение по умолчанию

По умолчанию установлено значение 1476.

Указания по использованию

Данная команда позволяет определить размер MTU (Maximum Transfer Unit) для инкапсулированных пакетов, передаваемых по туннелю.

Данное значение MTU применяется к пакетам, встроенным в протокол инкапсуляции; это значение не относится к пакетам транспортного протокола. Для пакетов транспортного протокола размер MTU зависит от физического интерфейса, передающего и принимающего пакеты.

Форма **set** данной команды используется для установки значения MTU для инкапсулированных пакетов

Форма **delete** данной команды используется для удаления настройки и восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки MTU для инкапсулированных пакетов.

2.10. interfaces tunnel <tunx> multicast <режим>

Установка режима передачи пакетов многоадресной рассылки через туннель.

Синтаксис

```
set interfaces tunnel <tunx> multicast <режим>
delete interfaces tunnel <tunx> multicast
show interfaces tunnel <tunx> multicast
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    tunnel tunx {
        multicast [enable|disable]
    }
```

```
}
```

Параметры

tunx

Обязательный. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от tun0 до tun999.

режим

Необязательный. Режим передачи многоадресного трафика через туннель. Допустимые значения:

- **enable**: включение режима передачи многоадресного трафика через туннель;
- **disable**: отключение режима передачи многоадресного трафика через туннель.

Значение по умолчанию

Режим передачи многоадресного трафика через туннель выключен.

Указания по использованию

Данная команда используется для включения/выключения режима передачи многоадресного трафика через туннель.

Форма **set** данной команды используется для включения/отключения режима передачи многоадресного трафика через туннель.

Форма **delete** данной команды используется для удаления настройки и восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки.

2.11. interfaces tunnel <tunx> remote-ip <ipv4-адрес>

Указание IP-адреса удаленного оконечного узла туннеля.

Синтаксис

```
set interfaces tunnel <tunx> remote-ip <ipv4-адрес>
delete interfaces tunnel <tunx> remote-ip
show interfaces tunnel <tunx> remote-ip
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    tunnel tunx {
        remote-ip ipv4-адрес
    }
}
```

Параметры

tunx

Обязательный. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от tun0 до tun999.

ipv4-адрес

Обязательный. IPv4-адрес оконечного узла туннеля на удаленном маршрутизаторе. IP-адрес должен быть заранее настроен на интерфейсе.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания IP-адреса удаленной оконечной точки туннеля.

Форма **set** данной команды используется для указания адреса удаленной оконечной точки туннеля.

Форма **delete** данной команды используется для удаления настройки удаленной оконечной точки туннеля. Для обеспечения работы туннеля необходимо настроить обе оконечные точки туннеля.

Форма **show** данной команды используется для отображения настройки удаленного оконечного узла туннеля.

2.12. interfaces tunnel <tunx> ttl <значение>

Указание значения TTL, которое будет записано в заголовок транспортного пакета IP.

Синтаксис

```
set interfaces tunnel <tunx> ttl <значение>
delete interfaces tunnel <tunx> ttl
show interfaces tunnel <tunx> ttl
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
interfaces {
    tunnel tunx {
        ttl 0-255
    }
}
```

Параметры

tunx

Обязательный. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от tun0 до tun999.

значение

Необязательный. Значение поля TTL, которое будет указано в заголовке IP транспортного пакета (пакета «носителя»). Значение должно лежать в диапазоне от 0 до 255, где 0 означает, что значение будет скопировано из пакета, который инкапсулируется.

Значение по умолчанию

По умолчанию установлено значение 255.

Указания по использованию

Данная команда позволяет указать значение поля TTL, указываемое в заголовке транспортного пакета IP. Поле TTL в заголовке пакета IP используется для ограничения времени жизни пакета.

Форма **set** данной команды используется для указания значения поля TTL, указываемого в заголовке IP транспортного пакета.

Форма **delete** данной команды используется для восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки поля TTL.

2.13. clear interfaces tunnel counters

Очистка статистической информации для туннельных интерфейсов.

Синтаксис

```
clear interfaces tunnel <tunx> counters
```

Режим интерфейса

Эксплуатационный режим.

Параметры

tunx

Необязательный. Очистка сведений для указанного туннельного интерфейса. Значение должно лежать в диапазоне от tun0 до tun999.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для очистки статистических сведений для туннельных интерфейсов. Просмотреть значения счетчиков можно при помощи команды **show interfaces counters**.

2.14. show interfaces tunnel

Вывод сведений для туннельных интерфейсов.

Синтаксис

```
show interfaces tunnel <tunx> [brief | detail]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

tunx

Необязательный. Вывод сведений для указанного туннельного интерфейса. Значение должно лежать в диапазоне от tun0 до tun999.

brief

Необязательный. Отображение кратких сведений для указанного туннеля.

detail

Необязательный. Отображение детализированных сведений для туннельных интерфейсов.

Значение по умолчанию

Вывод сведений для всех туннельных интерфейсов.

Указания по использованию

Данная команда используется для вывода состояния управления и работоспособности туннельного интерфейса.

Примеры

В примере 5 приведен вывод сведений о состоянии туннельного интерфейса tun0, использующего протокол GRE.

Пример 5 – «show interfaces tunnel»: отображение настройки туннеля

```
admin@edge:~$show interfaces tunnel

tun0@NONE: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1476 qdisc noqueue link/gre
192.168.20.2 peer 192.168.20.3

inet 192.168.20.1/24 brd 192.168.20.255 scope global tun0

RX: bytes packets errors dropped overrunmcast
```

```
0 0 0 0 0 0

TX: bytes packets errors dropped carriercollisions

0 0 0 0 0 0
```

Межсетевой экран Numa Edge

Руководство администратора

Настройка SOCKS proxy

Листов 23

Санкт-Петербург
2022

СОДЕРЖАНИЕ

ИДЕНТИФИКАЦИЯ ДОКУМЕНТА

Название документа	Руководство администратора. Настройка SOCKS proxy
Версия документа	1.0.1
Обозначение документа	643.АМБН.00004-01 32 06
Идентификация ОО	Межсетевой экран Numa Edge
Идентификация разработчика	ООО «НумаТех»
Ключевые слова	Межсетевой экран, МЭ, socksproxy

1. ВВЕДЕНИЕ

SOCKS – это интернет протокол, который используется для передачи данных от клиента к серверу с использованием посредника, называемого прокси-сервер. SOCKS версии 5 одобрен организацией IETF (Internet Engineering Task Force) в качестве стандарта Internet и включен в RFC 1928. Согласно IANA (Internet Assigned Numbers Authority), за протоколом SOCKS закреплен порт 1080 TCP/UDP.

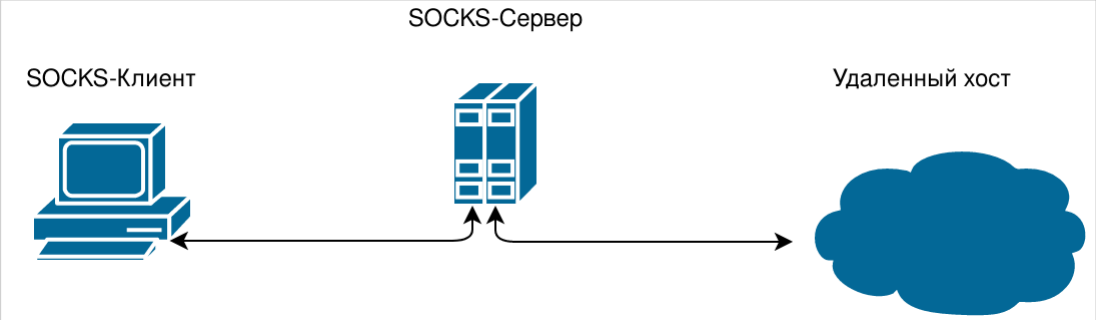


Рисунок 1 – Схема посредничества SOCKS-сервера при установлении соединения

Поскольку протокол SOCKS v5 концептуально является «промежуточным уровнем» между прикладным уровнем и транспортным уровнем, для передачи данных он использует TCP и UDP. Данная особенность позволяет использовать прокси-сервер в качестве посредника при передаче пакетов любого протокола прикладного уровня. При этом SOCKS-прокси никогда не изменяют заголовки пакетов с данными, что случается при использовании прокси других типов. Согласно спецификации протокола SOCKS различают SOCKS-сервер, который присутствует в Numa Edge в узле конфигурации *service socksproxy*, и SOCKS-клиент, который устанавливают на каждый пользовательский компьютер. SOCKS-сервер обеспечивает взаимодействие с любым прикладным сервером от имени соответствующего этому серверу прикладного клиента. SOCKS-клиент предназначен для перехвата всех запросов к прикладному серверу со стороны клиента и передачи их SOCKS-серверу. Следует отметить, что SOCKS-клиенты в большинстве своем встроены в различное сетевое ПО, такое как браузеры, почтовые клиенты, мессенджеры и т. д.

Каждое SOCKS-соединение проходит стадию аутентификации, если она требуется, затем клиент посылает команду. Команда может быть одна из трех:

- CONNECT – установить исходящее соединение с удаленным хостом по указанному TCP-порту и IP-адресу;
- BIND – открыть TCP порт, используется для TCP соединений, установленных после команды CONNECT. Применяется для протоколов, которые требуют, чтобы клиент принимал соединения со стороны удаленного хоста. Хорошим примером является FTP, которому для передачи данных необходимо знать, какой порт клиента использовать для установления соединения со стороны сервера;
- UDP ASSOCIATE – открыть UDP порт, в ответном сообщении сервер указывает IP-адрес и UDP-порт, на которые следует направлять исходящие датаграммы.

В ответ на эти сообщения SOCKS-сервер отправляет ответы BIND REPLY для протокола TPC и UDP REPLY для протокола UDP, которые соответствуют успешному выполнению команды на сервере.

SOCKS-сервер позволяет контролировать установление соединения клиента с удаленным хостом в трех этапах:

Во время промежуточного соединения с SOCKS-сервером, при получении команд CONNECT и UDP ASSOCIATE от клиента, по указанному IP-адресу клиента, его порту (только для TCP) и имени пользователя

Во время прохождения аутентификации по имени пользователя и пароле, предоставленным клиентом.
Для операций BIND и UDPASSOCIATE, когда удаленный хост пытается подключиться или отправить пакет UDP SOCKS-клиенту.

2. ПРИМЕРЫ НАСТРОЙКИ

В примерах ниже рассматриваются различные сценарии использования SOCKS-сервера.

2.1. Анонимный SOCKS-сервер

Классическим применением протокола SOCKS, является сокрытие IP-адреса SOCKS-клиента при подключении к удаленному хосту. В этом случае не требуется авторизация пользователей, а интерфейс/адрес внешнего интерфейса SOCKS-сервера и внутреннего - одинаковые.

Данный пример может быть актуальным при использовании внешнего статического IP-адреса на Numa Edge. Также в данном примере не будет использоваться аутентификация пользователей.

В описанном ниже примере считается, что на интерфейсе eth0 используется статический IP-адрес 203.0.113.1/24 из диапазона сети, выданной провайдером.

Пример 1 – Настройка анонимного SOCKS-сервера на S1

Действие	**Команда**
Указываем адрес, на который будут подключаться клиенты, порт по умолчанию 1080.	`[edit]` `admin@S1#set service socksproxy internal address 203.0.113.1`
Указываем интерфейс, с которого SOCKS-сервер будет осуществлять подключения к внешним хостам	`[edit]` `admin@S1#set service socksproxy external interface eth0`
Фиксация изменений.	`[edit]` `admin@S1# commit`

Вывод настроек socksproxy	`[edit]`
	`admin@S1#show service socksproxy`
	`external {`
	`  interface eth0`
	`}`
	`internal {`
	`  address 203.0.113.1`
	`}`

Примечание. Допускаются все возможные комбинации использования адресов или интерфейсов в узле конфигурации service socksproxy [internal|external], например, использование интерфейса eth0 в качестве внешнего и внутреннего интерфейса.

После применения данных настроек на SOCKS-клиенте необходимо указать адрес SOCKS-сервера 203.0.113.1 и порт 1080.

2.2. Цепочка SOCKS-серверов

При использовании socksproxy допускается построение неограниченных цепочек SOCKS-серверов, когда один SOCKS-сервер перенаправляет пакеты на другой SOCKS-сервер.

Настроим еще один SOCKS-сервер со статическим адресом 192.51.100.1/24.

Пример 2 – Настройка SOCKS-сервера на S2

Действие	**Команда**
Указываем адрес, на который будут подключаться клиенты, порт по умолчанию 1080	`[edit]` `admin@S2#set service socksproxy internal address 192.51.100.1`
Указываем адрес, с которого SOCKS-сервер будет осуществлять подключения к внешним хостам	`[edit]` `admin@S2#set service socksproxy external address 192.51.100.1`
Фиксация изменений	`[edit]`

Действие	Команда
	admin@S2# commit

Вывод настроек socksproxy	[edit]
	admin@S2#show service socksproxy
	external {
	address 192.51.100.1
	}
	internal {
	address 192.51.100.1
	}

Теперь добавим на S1 адрес SOCKS-сервера S2 для создания цепочки серверов.

Пример 3 – Добавление второго SOCKS-сервера в цепочку на S1

Действие	Команда
Указываем адрес, на который будут подключаться клиенты, порт по умолчанию 1080	[edit] admin@S1#set service socksproxy chaining 192.51.100.1
Фиксация изменений	[edit] admin@S1# commit

Вывод настроек socksproxy	[edit]
	admin@S1#show service socksproxy
	chaining{
	address 192.51.100.1
	}
	external {
	interface eth0
	}
	internal {
	address 203.0.113.1
	}

2.3. SOCKS-сервер с авторизацией и разграничением прав доступа во внешнюю сеть.

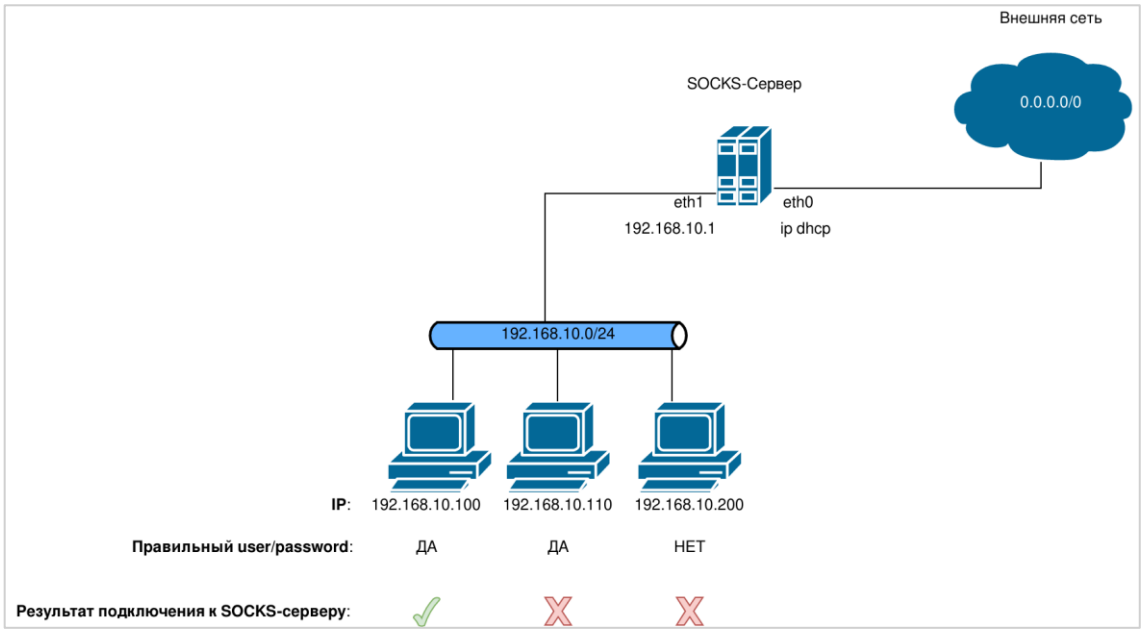


Рисунок 2 – Схема настройки

В этом примере будет рассматриваться SOCKS-сервер внутри локальной сети с ограничением доступа во внешнюю сеть на основе IP-адреса источника при его успешной аутентификации.

Предположим, что есть локальная сеть, внутри которой расположен SOCKS-сервер с IP-адресом 192.168.10.1/24. В этой же локальной сети находятся ПК клиентов, на сетевом ПО которых настроено подключение с SOCKS-серверу.

Сетевое ПО клиентов поддерживает аутентификацию согласно стандарту RFC 1929. Необходимо обеспечить возможность управлять доступом клиентов во внешнюю сеть согласно аутентификации и IP-адресу клиента.

Пример 4 - Настройка SOCKS-сервера

Действие	**Команда**
Указываем в качестве внешнего интерфейса SOCKS-сервера eth0	`[edit]` `admin@server#set service socksproxy external interface eth0`
Указываем, что SOCKS-сервер будет ожидать подключения клиентов на адресе 192.168.10.1	`[edit]` `admin@server#set service socksproxy internal address 192.168.10.1`
Создаем правило подключения клиентов, в котором указываем что клиенты могут подключаться только из локальной сети	`[edit]` `admin@server#set service socksproxy access-rules client 1 address 192.168.10.0/24`
Разрешаем описанное выше правило, подключение с других IP-адресов будет запрещено	`[edit]` `admin@server#set service socksproxy access-rules client 1 action permit`
Указываем метод аутентификации пользователей по логину и паролю	`[edit]` `admin@server#set service socksproxy authentication method users`
Указываем пользователя, которому разрешено подключатся к SOCKS-серверу	`[edit]` `admin@server#set service socksproxy authentication users test password testpassword`
Разрешаем SOCKS-серверу перенаправлять пакеты на любой удаленный хост	`[edit]` `admin@server#set service socksproxy access-rules socks 1 destination address 0.0.0.0/0`
Разрешаем подключение к SOCKS-серверу только SOCKS-клиенту с адресом 192.168.10.100	`[edit]` `admin@server#set service socksproxy access-rules socks 1 source address 192.168.10.100`
Разрешаем описанное выше правило	`[edit]` `admin@server#set service socksproxy access-rules socks 1 action permit`
Фиксация изменений	`[edit]` `admin@S1# commit`

Вывод настроек socksproxy	`admin@server# show service socksproxy`
	`access-rules {`
	`client 1 {`
	`action permit`
	`address 192.168.10.0/24`
	`}`
	`socks 1 {`
	`action permit`
	`destination {`
	`address 0.0.0.0/0`
	`}`

Действие	Команда

	source {
	address 192.168.10.100
	}
	}
	}
	authentication {
	method users
	users test {
	password testpassword
	}
	}
	external {
	interface eth0
	}
	internal {
	address 192.168.10.1
	}

Для разрешения доступа во внешнюю сеть другим клиентам необходимо создать правило, аналогичное *access-rules socks 1* с другим номером, в котором в качестве *source address* - указать IP-адрес клиента.

Примечание. Обратите внимание, что при использовании данного метода аутентификации, имя пользователя и пароль будут передаваться в открытом виде. Numa Edge поддерживает также метод аутентификации GSS-API, описанный в стандарте RFC 1961 для более безопасной передачи имени пользователя и пароля.

3. КОМАНДЫ НАСТРОЙКИ

В данном разделе описаны команды настройки SOCKS proxy, поддерживаемые Numa Edge.
В данном разделе приведены следующие команды:

Команды настройки	
service socksproxy	Конфигурация SOCKS proxy-сервера.
service socksproxy access-rules client <номер_правила>	Определение правила доступа к SOCKS-серверу.
service socksproxy access-rules client <номер_правила> action <действие>	Указание действия, которое должно быть выполнено для пакетов, соответствующих правилу доступа к SOCKS-серверу.
service socksproxy access-rules client <номер_правила> address <адрес>	Указание адреса SOCKS-сервера.
service socksproxy access-rules client <номер_правила> domain <домен>	Указание домена или хоста SOCKS-сервера.
service socksproxy access-rules client <номер_правила> port <порт>	Указание порта или диапазона портов SOCKS-сервера.
service socksproxy access-rules socks <номер_правила>	Определение правила доступа ко внешним ресурсам.
service socksproxy access-rules socks <номер_правила> action <действие>	Указание действия, которое должно быть выполнено для пакетов, соответствующих правилу доступа ко внешним ресурсам.
service socksproxy access-rules socks <номер_правила> command <команда>	Указание команды, которая должна быть выполнена для пакетов, соответствующих правилу доступа ко внешним ресурсам.
service socksproxy access-rules socks <номер_правила> destination	Указание адреса, домена и номера сетевого порта получателя.
service socksproxy access-rules socks <номер_правила> source	Указание адреса, домена и номера сетевого порта отправителя.
service socksproxy authentication method <режим_аутентификации>	Выбор режима аутентификации.
service socksproxy chaining	Перенаправление на другой SOCKS-сервер.
service socksproxy external	Указание внешнего адреса/интерфейса сервера для пересылки запросов.
service socksproxy internal	Указание внутреннего адреса/интерфейса сервера для обработки запросов клиентов.

3.1. service socksproxy

Конфигурация SOCKS proxy-сервера.

Синтаксис

```
set service socksproxy
delete service socksproxy
show service socksproxy
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   socksproxy {
```

```
    }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для включения сервера socksproxy в Numa Edge.

Форма **set** данной команды используется для включения сервера socksproxy в МЭ Numa Edge.

Форма **delete** данной команды используется для отключения режима сервера socksproxy в МЭ Numa Edge.

Форма **show** используется для отображения настройки.

3.2. service socksproxy access-rules client <номер_правила>

Определение правила доступа к SOCKS-серверу.

Синтаксис

```
set service socksproxy access-rules client <номер_правила>
delete service socksproxy access-rules client [<номер_правила>]
show service socksproxy access-rules client [<номер_правила>]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   socksproxy {
      access-rules {
         client номер_правила {
         }
      }
   }
}
```

Параметры

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 999. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации **access-rules client**.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет определить правило доступа к SOCKS-серверу.

Набор правил доступа может включать в себя до 999 настраиваемых правил. Правила доступа исполняются в порядке следования их номеров, от наименьшего к наибольшему. Для того чтобы не прибегать к изменению номеров правил, хорошей практикой является указание номеров с шагом 10. Это позволяет оставить пространство, куда можно будет впоследствии добавить новые правила.

Форма **set** данной команды используется для создания или изменения правила доступа к SOCKS-серверу.

Форма **delete** данной команды используется для удаления правила доступа к SOCKS-серверу.

Форма **show** данной команды используется для отображения настройки правила доступа к SOCKS-серверу.

3.3. service socksproxy access-rules client <номер_правила> action <действие>

Указание действия, которое должно быть выполнено для пакетов, соответствующих правилу доступа к SOCKS-серверу.

Синтаксис

```
set service socksproxy access-rules client <номер_правила>
action <действие>
delete service socksproxy access-rules client <номер_правила> action
show service socksproxy access-rules client <номер_правила> action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   socksproxy {
      access-rules {
         client номер_правила {
            action {
              deny
              permit
            }
         }
      }
   }
}
```

Параметры

номер_правила

Номер определенного правила доступа.

action

Действие, которое следует предпринять для пакетов, соответствующих правилу. Допустимые значения:

- **deny**: пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений;
- **permit**: пакеты, соответствующие данному правилу, пересылаются.

Значение по умолчанию

Пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений.

Указания по использованию

Форма **set** этой команды используется для определения действия, выполняемого над пакетом, удовлетворяющим критериям соответствия в данном правиле.

Если действием в правиле является **deny**, то пакеты, удовлетворяющие критериям соответствия правила, игнорируются без каких-либо действий и сообщений. Если действием в правиле является **permit**, то пакеты, удовлетворяющие критериям соответствия правила, пересылаются.

Форма **delete** этой команды используется для восстановления действия по умолчанию над пакетами, удовлетворяющими критериям соответствия.

Форма **show** этой команды используется для отображения параметров действия данного правила.

3.4. service socksproxy access-rules client <номер_правила> address <ip-адрес>

Указание адреса SOCKS-сервера.

Синтаксис

```
set service socksproxy access-rules client <номер_правила>
address <адрес>
delete service socksproxy access-rules client <номер_правила> address
show service socksproxy access-rules client <номер_правила> address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   socksproxy {
      access-rules {
         client номер_правила {
            address адрес
         }
      }
   }
}
```

Параметры

номер_правила
Номер определенного правила доступа.
адрес
Адрес SOCKS-сервера. Допустимые форматы:

- **IP-адрес**: IP-адрес;
- **IP-адрес/префикс**: адрес сети, где 0.0.0.0/0 соответствует любой сети.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать адрес SOCKS-сервера.
Форма **set** данной команды позволяет указать или изменить адрес SOCKS-сервера.
Форма **delete** данной команды позволяет удалить настройку адреса SOCKS-сервера.
Форма **show** данной команды позволяет отобразить настройку адреса SOCKS-сервера.

3.5. service socksproxy access-rules client <номер_правила> domain <домен>

Указание домена или хоста SOCKS-сервера.

Синтаксис

```
set service socksproxy access-rules client <номер_правила>
domain <домен>
delete service socksproxy access-rules client <номер_правила> domain
show service socksproxy access-rules client <номер_правила> domain
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   socksproxy {
      access-rules {
         client номер_правила {
            domain домен
         }
      }
   }
}
```

Параметры

номер_правила
Номер определенного правила доступа.
домен
Домен или хост SOCKS-сервера.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать домен или хост SOCKS-сервера.

Форма **set** данной команды позволяет указать или изменить домен или хост SOCKS-сервера.

Форма **delete** данной команды позволяет удалить настройку домена или хоста SOCKS-сервера.

Форма **show** данной команды позволяет отобразить настройку домена или хоста SOCKS-сервера.

3.6. service socksproxy access-rules client <номер_правила> port <порт>

Указание порта или диапазона портов SOCKS-сервера.

Синтаксис

```
set service socksproxy access-rules client <номер_правила> port <порт>
delete service socksproxy access-rules client <номер_правила> port
show service socksproxy access-rules client <номер_правила> port
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   socksproxy {
      access-rules {
         client номер_правила {
            port порт
         }
      }
   }
}
```

Параметры

номер_правила
Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 999.
порт
Порт SOCKS-сервера.

Допустимые форматы:

- **имя_порта:** проверка соответствия по названию службы IP, например, http. Названия различных служб можно указать в файле **/etc/services**;
- **номер_порта:** проверка соответствия по номеру порта. Значение должно лежать в диапазоне от 1 до 65535;
- **начало–конец:** проверка соответствия по номеру порта из указанного диапазона; например, 1001–1005.

Можно использовать сочетание этих форматов, указав список, разделенный запятыми. Также можно указать отрицание для всего списка, указав перед ним восклицательный знак (“!”); например, !22,telnet,http,123,1001-1005.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать порт или диапазон портов SOCKS-сервера.

Форма **set** данной команды позволяет указать или изменить порт или диапазон портов SOCKS-сервера.

Форма **delete** данной команды позволяет удалить порт или диапазон портов SOCKS-сервера.

Форма **show** данной команды позволяет отобразить настройку.

3.7. service socksproxy access-rules socks <номер_правила>

Определение правила доступа ко внешним ресурсам.

Синтаксис

```
set service socksproxy access-rules socks <номер_правила>
delete service socksproxy access-rules socks [<номер_правила>]
show service socksproxy access-rules socks [<номер_правила>]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   socksproxy {
      access-rules {
         socks номер_правила {
         }
      }
   }
}
```

Параметры

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 999. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации **access-rules socks**.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет определить правило доступа ко внешним ресурсам.

Набор правил доступа может включать в себя до 999 настраиваемых правил. Правила доступа исполняются в порядке следования их номеров от наименьшего к наибольшему. Для того чтобы не прибегать к изменению номеров правил, хорошей практикой является указание номеров с шагом 10. Это позволяет оставить пространство, куда можно будет впоследствии добавить новые правила.

Форма **set** данной команды используется для создания или изменения правила доступа ко внешним ресурсам.

Форма **delete** данной команды используется для удаления правила доступа ко внешним ресурсам.

Форма **show** данной команды используется для отображения настройки правила доступа ко внешним ресурсам.

3.8. service socksproxy access-rules socks <номер_правила> action <действие>

Указание действия, которое должно быть выполнено для пакетов, соответствующих правилу доступа ко внешним ресурсам.

Синтаксис

```
set service socksproxy access-rules socks <номер_правила>
action <действие>
delete service socksproxy access-rules socks <номер_правила> action
show service socksproxy access-rules socks <номер_правила> action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   socksproxy {
      access-rules {
         socks номер_правила {
            action {
               deny
               permit
            }
         }
      }
   }
}
```

Параметры

номер_правила

Номер определенного правила доступа.

action

Действие, которое следует предпринять для пакетов, соответствующих правилу. Допустимые значения:

- **deny**: пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений;
- **permit**: пакеты, соответствующие данному правилу, пересылаются.

Значение по умолчанию

Пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений.

Указания по использованию

Форма **set** этой команды используется для определения действия, выполняемого над пакетом, удовлетворяющим критериям соответствия в данном правиле.

Если действием в правиле является **deny**, то пакеты, удовлетворяющие критериям соответствия правила, игнорируются без каких-либо действий и сообщений. Если действием в правиле является **permit**, то пакеты, удовлетворяющие критериям соответствия правила, пересылаются.

Форма **delete** этой команды используется для восстановления действия по умолчанию над пакетами, удовлетворяющими критериям соответствия.

Форма **show** этой команды используется для отображения параметров действия данного правила.

3.9. service socksproxy access-rules socks <номер_правила> command <команда>

Указание команды, которая должна быть выполнена для пакетов, соответствующих правилу доступа ко внешним ресурсам.

Синтаксис

```
set service socksproxy access-rules socks <номер_правила>
command <команда>
delete service socksproxy access-rules socks <номер_правила> command
show service socksproxy access-rules socks <номер_правила> command
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   socksproxy {
      access-rules {
         socks номер_правила {
            command команда
         }
      }
   }
}
```

Параметры

номер_правила

Номер определенного правила доступа.

команда

Команда, выполняемая для соответствующих пакетов. Допустимые значения:

- **bind:** команда соответствует запросам клиентов;
- **connect:** команда соответствует запросам клиентов;
- **udpreply:** команда соответствует ответам внешних ресурсов;
- **bindreply:** команда соответствует ответам внешних ресурсов;
- **udpassociate:** команда соответствует запросам клиентов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для определения команды, выполняемой над пакетом, удовлетворяющим критериям соответствия в данном правиле.

Форма **delete** этой команды используется для отмены действия команды.

Форма **show** этой команды используется для отображения параметров действия данного правила.

3.10. service socksproxy access-rules socks <номер_правила> destination

Указание адреса, домена и номера сетевого порта получателя.

Синтаксис

```
set service socksproxy access-rules socks <номер_правила> destination
[address <адрес> | domain <домен> | port <порт>]
delete service socksproxy access-rules socks <номер_правила>
destination [address | domain | port]
show service socksproxy access-rules socks <номер_правила>
destination [address | domain | port]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   socksproxy {
      access-rules {
         socks номер_правила {
            destination {
               address адрес
               domain домен
               port порт
            }
         }
      }
   }
}
```

Параметры

адрес

Адрес или подсеть. Допустимые форматы:

- **IP-адрес**: внутренний IP-адрес;
- **IP-адрес/префикс**: адрес сети, где 0.0.0.0/0 соответствует любой сети.

домен

Домен или имя хоста.

порт

Порт назначения для проверки соответствия. Поддерживаются следующие значения:

- **имя_порта:** проверка соответствия по названию службы IP, например, http. Названия различных служб можно указать в файле **/etc/services**;
- **номер_порта:** проверка соответствия по номеру порта. Значение должно лежать в диапазоне от 1 до 65535;
- **начало–конец:** проверка соответствия по номеру порта из указанного диапазона; например, 1001–1005.

Можно использовать сочетание этих форматов, указав список, разделенный запятыми. Также можно указать отрицание для всего списка, указав перед ним восклицательный знак («!»); например, !22,telnet,http,123,1001-1005.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать параметры получателя.

Форма **set** данной команды позволяет указать или изменить адрес, домен и номер сетевого порта получателя.

Форма **delete** данной команды позволяет удалить настройку адреса, домена и номера сетевого порта получателя.

Форма **show** данной команды позволяет отобразить настройку адреса, домена и номера сетевого порта получателя.

3.11. service socksproxy access-rules socks <номер_правила> source

Указание адреса, домена и номера сетевого порта отправителя.

Синтаксис

```
set service socksproxy access-rules socks <номер_правила> source
[address <адрес> | domain <домен> | port <порт>]
delete service socksproxy access-rules socks <номер_правила>
source [address | domain | port]
show service socksproxy access-rules socks <номер_правила>
source [address | domain | port]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   socksproxy {
      access-rules {
         socks номер_правила {
            source {
               address адрес
               domain домен
               port порт
            }
         }
      }
   }
}
```

Параметры

адрес

Адрес или подсеть. Допустимые форматы:

- **IP-адрес:** внутренний IP-адрес;
- **IP-адрес/префикс:** адрес сети, где 0.0.0.0/0 соответствует любой сети.

домен

Домен или имя хоста.

порт

Порт назначения для проверки соответствия. Поддерживаются следующие значения:

- **имя_порта:** проверка соответствия по названию службы IP, например, http. Названия различных служб можно указать в файле **/etc/services**;
- **номер_порта:** проверка соответствия по номеру порта. Значение должно лежать в диапазоне от 1 до 65535;
- **начало–конец:** проверка соответствия по номеру порта из указанного диапазона; например, 1001–1005.

Можно использовать сочетание этих форматов, указав список, разделенный запятыми. Также можно указать отрицание для всего списка, указав перед ним восклицательный знак («!»); например, !22,telnet,http,123,1001-1005.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать внутренний адрес, домен и номер сетевого порта отправителя.

Форма **set** данной команды позволяет указать или изменить адрес, домен и номер сетевого порта отправителя.

Форма **delete** данной команды позволяет удалить настройку адреса, домена и номера сетевого порта отправителя.

Форма **show** данной команды позволяет отобразить настройку адреса, домена и номера сетевого порта отправителя.

3.12. service socksproxy authentication method <режим_аутентификации>

Выбор режима аутентификации.

Синтаксис

```
set service socksproxy authentication method <режим_аутентификации>
delete service socksproxy authentication method
show service socksproxy authentication method
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   socksproxy {
      authentication method режим_аутентификации
   }
}
```

Параметры

режим_аутентификации

Устанавливает режим аутентификации. Возможные значения:

- **gssapi:** аутентификация GSSAPI;
- **none:** отсутствие аутентификации;
- **users:** аутентификация по имени/паролю пользователя.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать режим аутентификации.

Форма **set** данной команды позволяет указать режим аутентификации SOCKS proxy-сервера.

Форма **delete** данной команды позволяет удалить настройку режима аутентификации.

Форма **show** данной команды позволяет отобразить настройку режима аутентификации.

3.13. service socksproxy chaining

Перенаправление на другой SOCKS-сервер.

Синтаксис

```
set service socksproxy chaining [address <адрес> | port <порт>]
delete service socksproxy chaining [address <адрес> | port <порт>]
show service socksproxy chaining
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   socksproxy {
      chaining{
         address адрес
         port порт
      }
   }
}
```

Параметры

адрес

IP-адрес другого SOCKS-сервера.

порт

Проверка соответствия по номеру порта. Значение должно лежать в диапазоне от 1 до 65535.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет выполнить перенаправление на другой SOCKS-сервер.

Форма **set** данной команды позволяет выполнить перенаправление на другой SOCKS-сервер.

Форма **delete** данной команды позволяет отменить перенаправление на другой SOCKS-сервер.

Форма **show** данной команды позволяет отобразить настройку перенаправления на другой SOCKS-сервер.

3.14. service socksproxy external

Указание внешнего адреса/интерфейса сервера для пересылки запросов.

Синтаксис

```
set service socksproxy external [address <адрес> |
interface <интерфейс>]
delete service socksproxy external [address | interface ]
show service socksproxy external
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   socksproxy {
      external{
         address адрес
         interface интерфейс
      }
   }
```

```
}
```

Параметры

адрес
Внешний IP-адрес.
интерфейс
Внешний интерфейс.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания внешнего адреса/интерфейса сервера для пересылки запросов. Параметры address/interface являются взаимоисключающими и, хотя бы один из них должен быть задан.

Форма **set** данной команды позволяет выполнить указание внешнего адреса/интерфейса сервера для пересылки запросов.

Форма **delete** данной команды позволяет отменить указание внешнего адреса/интерфейса сервера для пересылки запросов.

Форма **show** данной команды позволяет отобразить настройку внешнего адреса/интерфейса сервера для пересылки запросов.

3.15. service socksproxy internal

Указание внутреннего адреса/интерфейса сервера для обработки запросов клиентов.

Синтаксис

```
set service socksproxy internal [address <адрес> |
interface <интерфейс> | port <порт>]
delete service socksproxy internal [address | interface | port]
show service socksproxy internal [address | interface | port]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   socksproxy {
      internal{
         address адрес
         interface интерфейс
         port порт
      }
   }
}
```

Параметры

адрес
Внутренний IP-адрес. Допустимые форматы:

- IP-адрес: внутренний IP-адрес.

интерфейс
Внутренний интерфейс.
порт
Внутренний порт. Значение должно лежать в диапазоне от 1 до 65535.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания внутреннего адреса/интерфейса сервера для обработки запросов клиентов.

Форма **set** данной команды позволяет выполнить указание внутреннего адреса/интерфейса сервера для обработки запросов клиентов.

Форма **delete** данной команды позволяет отменить указание внутреннего адреса/интерфейса сервера для обработки запросов клиентов.

Форма **show** данной команды позволяет отобразить настройку внутреннего адреса/интерфейса сервера для обработки запросов клиентов.

Межсетевой экран Numa Edge

Руководство администратора

Настройка LVS

Листов 25

Санкт-Петербург
2022

ИДЕНТИФИКАЦИЯ ДОКУМЕНТА

Название документа	Руководство администратора. Настройка LVS
Версия документа	1.1
Идентификация ОО	Межсетевой экран Numa Edge
Идентификация разработчика	ООО «НумаТех»
Ключевые слова	Межсетевой экран, МЭ, LVS

1. ВВЕДЕНИЕ

Функционал LVS (Linux Virtual Server) в Numa Edge реализует возможность балансировки трафика на транспортном уровне модели OSI, используя заданные критерии. В терминологии LVS сам Numa Edge выступает в роли балансировщика нагрузки, а устройства, на которые производится балансировка — реальными серверами. А вместе они представляют собой для внешнего клиента один «виртуальный сервер».

Где и для чего применяется LVS:

- для увеличения пропускной способности, в том случае когда линейный прирост за счет добавления реальных серверов целесообразнее модернизации;
- для резервирования. Отдельные машины могут быть отключены от LVS, модернизированы и возвращены к работе без прерывания обслуживания клиентов. Машины могут перемещаться на новую площадку и подключаться к сети по одной, в то время как машины удаляются со старой площадки без прерывания обслуживания клиентов;
- для адаптивности. Если предполагается, что пропускная способность будет меняться постепенно или быстро, количество серверов можно увеличить (или уменьшить) прозрачно для клиентов.

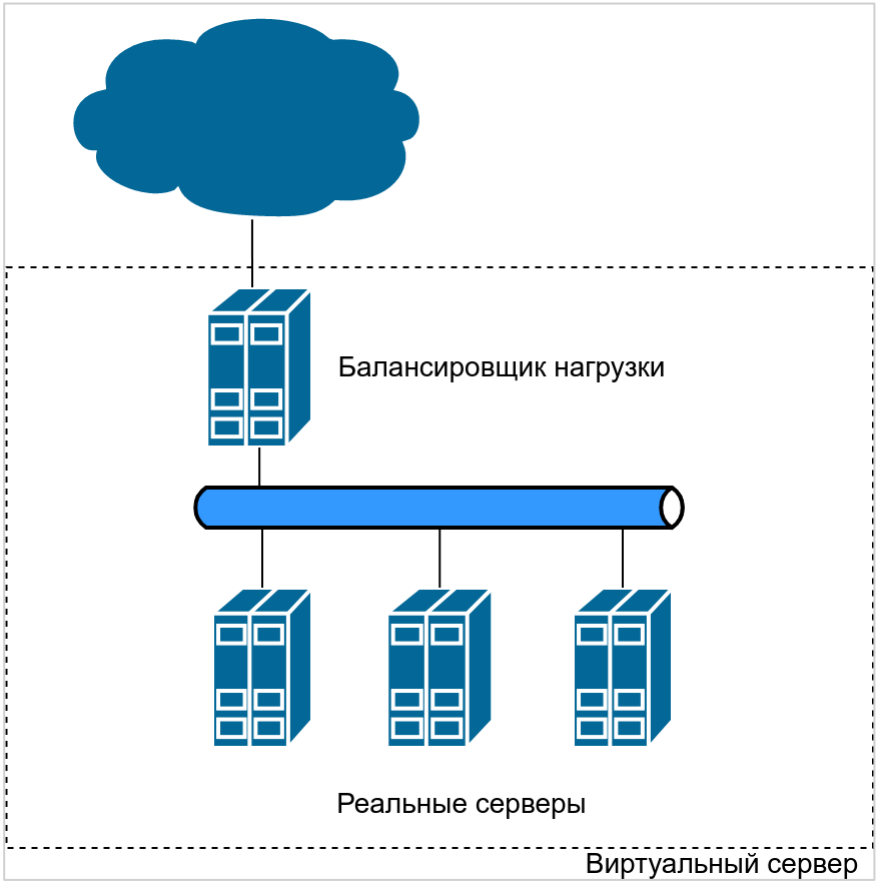


Рисунок 1 – Схема компонентов виртуального сервера

Балансировщик нагрузки предоставляет клиентам Виртуальный IP-адрес (VIP). VIP – это тот адрес, на котором производится балансировка нагрузки между реальными серверами. Необходимо иметь ввиду, что балансировка осуществляется на транспортном уровне. Ввиду этого, если «сервисом» выступает какой-либо веб-интерфейс (443/TCP), то балансировка производится только для трафика с адресом назначения равном VIP-адресу и портом назначения 443/TCP. При этом в случайный момент времени нельзя сказать, какой именно реальный сервер ответит запрос. При попытке доступа к VIP-адресу с использованием другого порта назначения и протокола, ответ

балансировщика будет зависеть от значения атрибута accept-mode в конфигурации VRRP и правил фильтрации. Принимая во внимание вышесказанное, для доступа к определенному реальному серверу или балансировщику трафика не рекомендуется использовать VIP-адрес.

Не трудно заметить, что «точкой отказа» в организации виртуального сервера является балансировщик нагрузки. С выходом его из строя схема перестает работать. В качестве меры, направленной на устранение этой проблемы, в Numa Edge в качестве виртуального IP-адреса LVS требуется указывать только ранее сконфигурированный виртуальный адрес VRRP. Это позволяет быстро организовать резервирование балансировщика нагрузки.

2. ПРИМЕР НАСТРОЙКИ

Рассмотрим пример, в рамках которого обеспечивается доступ к веб-сайту с использованием LVS с организацией резервирования балансировщика нагрузки.

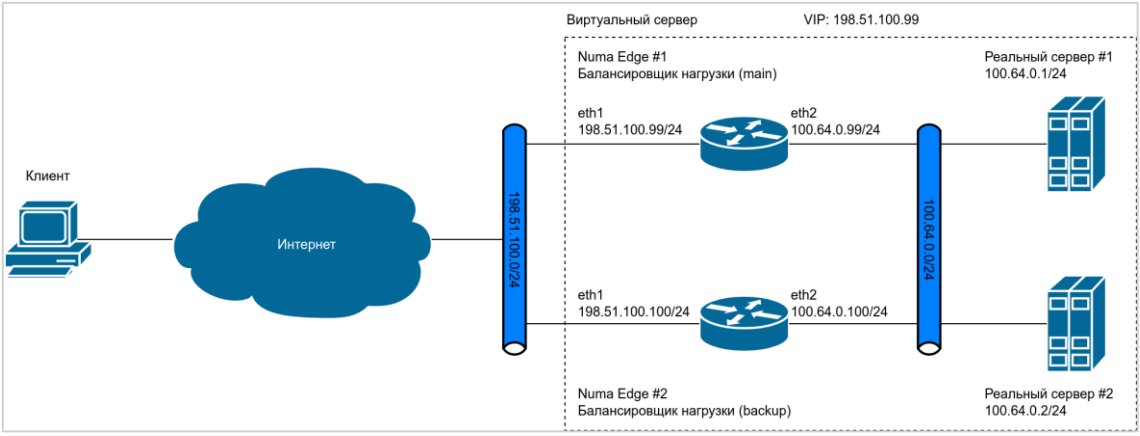


Рисунок 2 – – Схема LVS сервера с Numa Edge в качестве балансировщика нагрузки

В данном примере клиент подключается к виртуальному серверу из внешней сети (виртуальный IP-адрес которого 198.51.100.99). Далее Numa Edge, выступающий в роли балансировщика нагрузки, распределяет запросы на несколько имеющихся реальных серверов. В качестве метода переадресации будем использовать NAT, как самый простой в настройке вариант, не требующий дополнительных действий на реальных серверах.

В рамках примера не будем рассматривать настройку адресации на физических интерфейсах и преднастройку VRRP.

Пример 1 – Настройка LVS с резервированием балансировщика нагрузки

Узел: Numa Edge #1	
Действие	Команда

Вывод настроек VRRP на интерфейсах.
• Настроен VRRP на внешнем интерфейсе eth1, виртуальный адрес которого и будет являться VIP адресом сервиса LVS.
• Для VRRP на внешнем интерфейсе eth1 включен режим accept-mode, что позволяет устройству обрабатывать и отвечать на запросы, направляемые на VIP адрес, что необходимо для LVS.
• Настроен VRRP на внутреннем интерфейсе eth2 в сторону реальных серверов, виртуальный адрес которого будет использоваться для получения ответов. Рекомендуется использовать в случае резервирования балансировщика когда используется метод переадресации NAT.
• Задан повышенный приоритет для групп VRRP, так как это основной балансировщик, а
	[edit]
	admin@edge1# show interfaces ethernet eth1 vrrp
	1 {
	accept-mode true
	virtual-address 198.51.100.99
	priority 254
	sync-group MAIN-LB
	}
	[edit]
	admin@edge1# show interfaces ethernet eth2 vrrp
	1 {
	virtual-address 100.64.0.99
	priority 254
	sync-group MAIN-LB

Узел: Numa Edge #1	
также настроена синхронизация состояний VRRP интерфейсов.	}
Укажем в качестве адреса виртуального сервера ранее заданный виртуальный адрес VRRP на внешнем интерфейсе.	[edit] admin@edge1# set service lvs virtual-server 192.168.152.99
Перечислим имеющиеся реальные серверы для LVS.	[edit] admin@edge1# set service lvs virtual-server 192.168.152.99 real-server 100.64.0.1 [edit] admin@edge1# set service lvs virtual-server 192.168.152.99 real-server 100.64.0.2
Зададим сервис виртуального сервера. Так как мы настраиваем доступ к веб-ресурсу, укажем 'https'.	[edit] admin@edge1# set service lvs virtual-server 192.168.152.99 service https
Добавим проверку доступности реальных серверов в составе LVS с целью исключить ситуацию, когда реальный сервер вышел из строя или недоступен, а клиенты на него пересылаются.	[edit] admin@edge1# set service lvs virtual-server 192.168.152.99 check type https-head
Укажем группу VRRP, которая будет использоваться для синхронизации.	[edit] admin@edge1# set service lvs sync id 1
Укажем интерфейс, на котором будет происходить синхронизация с дублирующим балансировщком.	[edit] admin@edge1# set service lvs sync interace eth2
Фиксация изменений.	[edit] admin@edge1# commit

Вывод настроек LVS.	admin@edge-fw1# show service lvs
	sync {
	id 1
	interface eth4
	}
	virtual-server 198.51.100.99 {
	check {
	type https-head
	}
	real-server 100.64.0.1 {

Узел: Numa Edge #1	

	}
	real-server 100.64.0.2 {
	}
	service https
	}

Примечание. При использовании других методов переадресации (DR и Tunnel) потребуется подготовить реальные серверы, выполнив на них ряд дополнительных настроек.

Настройка LVS на дублирующем Numa Edge #2 не отличается от основного. Отличается адресация на физических интерфейсах (задается в соответствии со схемой примера) и приоритет устройства для групп VRRP оставлен в значении по умолчанию. После реализации такой схемы, при отказе основного балансировщика, его функции продолжит выполнять дублирующий.

В результате должна получиться следующая конфигурация.

Действие	**Команда**

Полученная конфигурация интерфейсов.	[edit]
	admin@edge1# show interfaces ethernet eth1 vrrp
	1 {
	accept-mode true
	virtual-address 198.51.100.99
	priority 254
	sync-group MAIN-LB
	}
	[edit]
	admin@edge1# show interfaces ethernet eth2 vrrp
	1 {
	virtual-address 100.64.0.99
	priority 254
	sync-group MAIN-LB
	}

Полученная конфигурация сервиса LVS.	admin@edge-fw1# show service lvs
	sync {
	id 1
	interface eth4
	}
	virtual-server 198.51.100.99 {

Действие	**Команда**

	check {
	type https-head
	}
	real-server 100.64.0.1 {
	}
	real-server 100.64.0.2 {
	}
	service https
	}

3. КОМАНДЫ НАСТРОЙКИ LVS

В данном разделе описаны команды настройки LVS, поддерживаемые Numa Edge.

Команды настройки	
service lvs	Конфигурация виртуального сервера
service lvs sync id <идентификатор>	Указание идентификатора группы VRRP для синхронизации виртуального сервера
service lvs sync interface <интерфейс>	Указание интерфейса, используемого для синхронизации виртуального сервера
service lvs virtual-address <ip-адрес>	Указание адреса виртуального сервера
service lvs virtual-address <ip-адрес> forwarding-method <тип_переадресации>	Указание метода переадресации, используемого для входящих соединений
service lvs virtual-address <ip-адрес> check delay-loop <временной_интервал>	Указание интервала времени между выполнением проверок доступности
service lvs virtual-address <ip-адрес> check delay-retry <временной_интервал>	Указание времени между повторными проверками при восстановлении доступности реального сервера
service lvs virtual-address <ip-адрес> check http-resource <ресурс>	Указание запрашиваемого http-ресурса на реальном сервере
service lvs virtual-address <ip-адрес> check retry <количество_проверок>	Указание количества успешных проверок для принятия решения о доступности реального сервера
service lvs virtual-address <ip-адрес> check timeout <временной_интервал>	Указание максимального времени ожидания ответа от реального сервера при проведении проверки доступности
service lvs virtual-address <ip-адрес> check type <тип_проверки>	Указание используемой проверки реальных серверов
service lvs virtual-address <ip-адрес> proto <протокол>	Указание протокола, используемого для переадресации трафика
service lvs virtual-address <ip-адрес> real-server <ip-адрес>	Указание адреса реального сервера, на который будет выполняться переадресация
service lvs virtual-address <ip-адрес> real-server <ip-адрес> lower-treshold <число_подключений>	Указание минимального количества подключений к определенному реальному серверу
service lvs virtual-address <ip-адрес> real-server <ip-адрес> service <сервис>	Указание сервиса или порта на определенном реальном сервере

Команды настройки	
service lvs virtual-address <ip-адрес> real-server <ip-адрес> upper-treshold <число_подключений>	Указание максимального количества подключений к определенному реальному серверу
service lvs virtual-address <ip-адрес> real-server <ip-адрес> weight <вес>	Указание веса для определенного реального сервера
service lvs virtual-address <ip-адрес> scheduler-algo <алгоритм>	Указание алгоритма распределения нагрузки по реальным серверам
service lvs virtual-address <ip-адрес> service <сервис>	Указание сервиса или порта виртуального сервера
Эксплуатационные команды	
service lvs show	Отображение сведений о состоянии сервиса LVS

3.1. service lvs

Конфигурация виртуального сервера.

Синтаксис

```
set service lvs
delete service lvs
show service lvs
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    lvs {
    }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для включения виртуального сервера в Numa Edge.
Форма **set** данной команды используется для включения виртуального сервера.
Форма **delete** данной команды используется для отключения виртуального сервера.
Форма **show** используется для отображения настройки.

3.2. service lvs sync id <идентификатор>

Указание идентификатора группы VRRP для синхронизации виртуального сервера.

Синтаксис

```
set service lvs sync id <идентификатор>
delete service lvs sync id [<идентификатор>]
show service lvs sync id
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   lvs {
      sync {
         id идентификатор
         }
      }
   }
}
```

Параметры

идентификатор
Номер группы VRRP, в которой выполняется синхронизация виртуального сервера.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для указания идентификатора группы VRRP, в рамках которой будет выполняться синхронизация виртуального сервера.

Форма **delete** этой команды используется для удаления идентификатора группы VRRP.

Форма **show** этой команды используется для отображения заданного идентификатора группы VRRP.

3.3. service lvs sync interface <интерфейс>

Указание интерфейса, используемого для синхронизации виртуального сервера.

Синтаксис

```
set service lvs sync interface <интерфейс>
delete service lvs sync interface [<интерфейс>]
show service lvs sync interface
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   lvs {
      sync {
         interface интерфейс
         }
      }
   }
}
```

Параметры

интерфейс
Интерфейс, на котором настроен VRRP и который будет использоваться для синхронизации виртуального сервера.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для указания интерфейса, используемого для синхронизации виртуального сервера.

Форма **delete** этой команды используется для удаления ранее указанного интерфейса.

Форма **show** этой команды используется для отображения заданного интерфейса.

3.4. service lvs virtual-address <ip-адрес>

Указание адреса виртуального сервера.

Синтаксис

```
set service lvs virtual-address <ip-адрес>
delete service lvs virtual-address [<ip-адрес>]
show service lvs virtual-address
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   lvs {
      virtual-address ip-адрес
   }
}
```

Параметры

ip-адрес

IPv4-адрес, указываемый в качестве адреса виртуального сервера.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для назначения виртуальному серверу IP-адреса.

В Numa Edge в качестве IP-адреса для виртуального сервера может быть назначен существующий виртуальный адрес VRRP. По этой причине предварительно необходимо выполнить настройку группы VRRP, используя команды соответствующего раздела «Руководства администратора» 643.АМБН.00004-01 32 01.

Форма **delete** данной команды используется для удаления IP адреса виртуального сервера.

Форма **show** используется для отображения адреса виртуального сервера.

3.5. service lvs virtual-address <ip-адрес> forwarding-method <тип_переадресации>

Указание метода переадресации, используемого для входящих соединений.

Синтаксис

```
set service lvs virtual-address <ip-адрес> forwarding-method
<тип_переадресации>
delete service lvs virtual-address <ip-адрес> forwarding-method
[<тип_переадресации>]
show service lvs virtual-address <ip-адрес> forwarding-method
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   lvs {
```

```
            virtual-address ip-адрес {
               forwarding-method тип_переадресации
            }
         }
      }
```

Параметры

ip-адрес

IPv4-адрес, указываемый в качестве адреса виртуального сервера.

тип_переадресации

Указывает механизм, который используется для переадресации пакетов на реальные серверы. Может принимать следующие значения:

- nat: используется трансляция адресов получателя (DNAT);
- dr: используется режим, в котором ответы от реального сервера пересылаются напрямую клиенту, выполняющему запрос, минуя балансировщик нагрузки;
- tun: используется режим, аналогичный предыдущему, однако в дополнение выстраивается туннель между реальным сервером и клиентом, выполняющим запрос.

Значение по умолчанию

По умолчанию в качестве типа переадресации используется трансляция адресов получателя (DNAT).

Указания по использованию

При использовании типов переадресации DR и Tunnel потребуется подготовить реальные серверы, выполнив на них ряд дополнительных настроек.

Форма **set** данной команды используется для указания используемого метода переадресации пакетов на реальный сервер.

Форма **delete** данной команды используется для восстановления значения по умолчанию.

Форма **show** используется для отображения используемого метода.

3.6. service lvs virtual-address <ip-адрес> check delay-loop <временной_интервал>

Указание интервала времени между выполнением проверок доступности.

Синтаксис

```
      set service lvs virtual-address <ip-адрес> check delay-loop
<временной_интервал>
      delete service lvs virtual-address <ip-адрес> check delay-loop
[<временной_интервал>]
      show service lvs virtual-address <ip-адрес> check delay-loop
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
      service {
         lvs {
            virtual-address ip-адрес {
               check {
                   delay-loop временной_интервал
               }
            }
         }
      }
```

Параметры

ip-адрес

IPv4-адрес, указываемый в качестве адреса виртуального сервера.

временной_интервал

Указывает промежуток времени в секундах между выполнением проверок доступности реальных серверов.

Значение по умолчанию

По умолчанию, если сконфигурирована проверка доступности, задается интервал в 60 секунд.

Указания по использованию

Форма **set** данной команды используется для указания временного интервала выполнения проверок доступности реальных серверов в составе LVS.

Форма **delete** данной команды используется для восстановления значения по умолчанию.

Форма **show** используется для отображения установленного временного интервала.

3.7. service lvs virtual-address <ip-адрес> check delay-retry <временной_интервал>

Указание времени между повторными проверками при восстановлении доступности реального сервера.

Синтаксис

```
set service lvs virtual-address <ip-адрес> check delay-retry <временной_интервал>
delete service lvs virtual-address <ip-адрес> check delay-retry [<временной_интервал>]
show service lvs virtual-address <ip-адрес> check delay-retry
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   lvs {
      virtual-address ip-адрес {
         check {
             delay-retry временной_интервал
         }
      }
   }
}
```

Параметры

ip-адрес

IPv4-адрес, указываемый в качестве адреса виртуального сервера.

временной_интервал

При восстановлении доступности реального сервера, прежде чем включить его в список доступных совершается цикл проверок доступности в количестве, определяемом командой `service lvs virtual-address <ip-адрес> check retry <количество>`, с целью убедиться в надёжности соединения. Данная команда указывает промежуток времени в секундах между выполнением проверок в цикле при восстановлении доступности реального сервера.

Значение по умолчанию

По умолчанию, если сконфигурирована проверка доступности, задается интервал в 3 секунды.

Указания по использованию

Форма **set** данной команды используется для указания временного интервала между проверками в цикле при восстановлении доступа к реальному серверу в составе LVS.

Форма **delete** данной команды используется для восстановления значения по умолчанию.

Форма **show** используется для отображения установленного временного интервала.

3.8. service lvs virtual-address <ip-адрес> check http-resource <ресурс>

Указание запрашиваемого http-ресурса на реальном сервере.

Синтаксис

```
set service lvs virtual-address <ip-адрес> check http-resource <ресурс>
delete service lvs virtual-address <ip-адрес> check http-resource [<ресурс>]
show service lvs virtual-address <ip-адрес> check http-resource
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   lvs {
      virtual-address ip-адрес {
         check {
             http-resource ресурс
         }
      }
   }
}
```

Параметры

ip-адрес

IPv4-адрес, указываемый в качестве адреса виртуального сервера.

ресурс

Множественный узел. Указывает запрашиваемый на реальном сервере http-ресурс для проверки.

Значение по умолчанию

По умолчанию в качестве ресурса запрашивается "/".

Указания по использованию

Данный механизм применим для проверок http-head и https-head. С помощью данной команды указываются http-ресурсы на реальном сервере, далее при применении конфигурации вычисляется хэш для указанных ресурсов. При проведении проверки сохраненный хэш сравнивается с вычисляемым. В случае несоответствия принимается решение о недоступности реального сервера.

Форма **set** данной команды используется для указания http-ресурса на реальном сервере для проверки доступности.

Форма **delete** данной команды используется для восстановления значения по умолчанию.

Форма **show** используется для отображения запрашиваемых http-ресурсов.

3.9. service lvs virtual-address <ip-адрес> check retry <количество_проверок>

Указание количества успешных проверок для принятия решения о доступности реального сервера.

Синтаксис

```
set service lvs virtual-address <ip-адрес> check retry
<количество_проверок>
delete service lvs virtual-address <ip-адрес> check retry
[<количество_проверок>]
show service lvs virtual-address <ip-адрес> check retry
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   lvs {
      virtual-address ip-адрес {
         check {
             retry количество_проверок
         }
      }
   }
}
```

Параметры

ip-адрес

IPv4-адрес, указываемый в качестве адреса виртуального сервера.

количество_проверок

Указывает количество успешных проверок реального сервера после восстановления доступа с целью убедиться в надёжности соединения.

Значение по умолчанию

По умолчанию, если сконфигурирована проверка доступности, задаются 3 проверки.

Указания по использованию

Форма **set** данной команды используется для указания количества проверок в цикле при восстановлении доступа к реальному серверу в составе LVS.

Форма **delete** данной команды используется для восстановления значения по умолчанию.

Форма **show** используется для отображения установленного количества успешных проверок.

3.10. service lvs virtual-address <ip-адрес> check timeout <временной_интервал>

Указание максимального времени ожидания ответа от реального сервера при проведении проверки доступности.

Синтаксис

```
set service lvs virtual-address <ip-адрес> check timeout
<временной_интервал>
delete service lvs virtual-address <ip-адрес> check timeout
[<временной_интервал>]
show service lvs virtual-address <ip-адрес> check timeout
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   lvs {
      virtual-address ip-адрес {
         check {
```

```
                timeout временной_интервал
            }
        }
    }
}
```

Параметры

ip-адрес

IPv4-адрес, указываемый в качестве адреса виртуального сервера.

временной_интервал

Указывает максимальный период ожидания ответа от реального сервера в секундах при выполнении проверки доступности.

Значение по умолчанию

По умолчанию, если сконфигурирована проверка доступности, интервал составляет 5 секунд.

Указания по использованию

Форма **set** данной команды используется для указания времени ожидания ответа от реального сервера при проведении проверки доступности.

Форма **delete** данной команды используется для восстановления значения по умолчанию.

Форма **show** используется для отображения установленного количества успешных проверок.

3.11. service lvs virtual-address <ip-адрес> check type <тип_проверки>

Указание используемой проверки реальных серверов.

Синтаксис

```
set service lvs virtual-address <ip-адрес> check type <тип_проверки>
delete service lvs virtual-address <ip-адрес> check type
[<тип_проверки>]
show service lvs virtual-address <ip-адрес> check type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    lvs {
        virtual-address ip-адрес {
            check {
                type тип_проверки
            }
        }
    }
}
```

Параметры

ip-адрес

IPv4-адрес, указываемый в качестве адреса виртуального сервера.

тип_проверки

Указывает проверку, которая будет применяться для реальных серверов в составе LVS. Может принимать следующие значения:

- http-head: Проверка путем выполнения http HEAD запроса к указанному http-ресурсу. Применима для сервиса http;

- https-head: Проверка путем выполнения https HEAD запроса к указанному http-ресурсу. Применима для сервиса https;
- icmp-ping: Проверка путем выполнения ICMP-request запросов до реальных серверов. Применима для любых сервисов. Может потребоваться донастройка реальных серверов, чтобы они отвечали на подобные запросы;
- tcp-check: Проверка путем установления TCP-соединения до реального сервера. Применима для сервисов, работающих по протоколу TCP. Подключение выполняется на порт, соответствующий настроенному сервису.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для указания используемой проверки доступности реальных серверов.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** используется для отображения используемой проверки.

3.12. service lvs virtual-address <ip-адрес> proto <протокол>

Указание протокола, используемого для переадресации трафика.

Синтаксис

```
set service lvs virtual-address <ip-адрес> proto <протокол>
delete service lvs virtual-address <ip-адрес> proto [<протокол>]
show service lvs virtual-address <ip-адрес> proto
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   lvs {
      virtual-address ip-адрес {
         proto протокол
      }
   }
}
```

Параметры

ip-адрес

IPv4-адрес, указываемый в качестве адреса виртуального сервера.

протокол

Протокол. Указывает какой транспортный протокол используется для переадресации на реальные серверы. Может принимать значения tcp или udp. Данный параметр выступает в роли фильтра, так как по умолчанию используемые протоколы формируются на основании указанного сервиса. Параметр следует применять в том случае, когда требуется ограничить используемый протокол транспортного уровня каким-либо конкретным.

Значение по умолчанию

По умолчанию используемый протоков выводится на основании указанного командой `set service lvs virtual-address <ip-адрес> service <сервис>` сервиса.

Если для сервиса возможен вариант использования как TCP, так и UDP, будут добавлены оба протокола. Если только какой-либо один, то будет использоваться он.

При этом в конфигурации значение по умолчанию не отображается, так как параметр используется в качестве ограничивающего фильтра.

Указания по использованию

Форма **set** данной команды используется для указания протокола для переадресации трафика.

Форма **delete** данной команды используется для восстановления значения по умолчанию.

Форма **show** используется для отображения используемого протокола.

3.13. service lvs virtual-address <ip-адрес> real-server <ip-адрес>

Указание адреса реального сервера, на который будет выполняться переадресация.

Синтаксис

```
set service lvs virtual-address <ip-адрес> real-server <ip-адрес>
delete service lvs virtual-address <ip-адрес> real-server [<ip-адрес>]
show service lvs virtual-address <ip-адрес> real-server [<ip-адрес>]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   lvs {
      virtual-address ip-адрес {
         real-server ip-адрес
      }
   }
}
```

Параметры

virtual-address ip-адрес

IPv4-адрес, указываемый в качестве адреса виртуального сервера.

real-server ip-адрес

IPv4-адрес реального сервера, на который будет выполняться переадресация.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для указания адреса реального сервера.

Форма **delete** данной команды используется для удаления настроек реального сервера.

Форма **show** используется для отображения настроек реального сервера.

3.14. service lvs virtual-address <ip-адрес> real-server <ip-адрес> lower-treshold <число_подключений>

Указание минимального количества подключений к определенному реальному серверу.

Синтаксис

```
set service lvs virtual-address <ip-адрес> real-server <ip-адрес> lower-treshold <число_подключений>
delete service lvs virtual-address <ip-адрес> real-server <ip-адрес> lower-treshold [<число_подключений>]
show service lvs virtual-address <ip-адрес> real-server <ip-адрес> lower-treshold
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   lvs {
      virtual-address ip-адрес {
         real-server ip-адрес {
             lower-treshold число_подключений
         }
      }
   }
}
```

Параметры

virtual-address ip-адрес

IPv4-адрес, указываемый в качестве адреса виртуального сервера.

real-server ip-адрес

IPv4-адрес реального сервера, на который будет выполняться переадресация.

число_подключений

Задает минимальное число подключений к указанному реальному серверу. Диапазон значений u32.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для указания минимального количества подключений к реальному серверу.

Форма **delete** данной команды используется для удаления значения минимального количества подключений.

Форма **show** используется для отображения минимального количества подключений к указанному реальному серверу.

3.15. service lvs virtual-address <ip-адрес> real-server <ip-адрес> service <сервис>

Указание порта на реальном сервере, на который будет выполняться переадресация.

Синтаксис

```
set service lvs virtual-address <ip-адрес> real-server <ip-адрес> service <сервис>
delete service lvs virtual-address <ip-адрес> real-server <ip-адрес> service [<сервис>]
show service lvs virtual-address <ip-адрес> real-server <ip-адрес> service
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   lvs {
      virtual-address ip-адрес {
         real-server ip-адрес {
             service сервис
         }
      }
   }
}
```

Параметры

virtual-address ip-адрес

IPv4-адрес, указываемый в качестве адреса виртуального сервера.

real-server ip-адрес

IPv4-адрес реального сервера, на который будет выполняться переадресация.

сервис

Имя сервиса или порт на реальном сервере, на который будет выполняться переадресация.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для указания сервиса или порта на реальном сервере.

Форма **delete** данной команды используется для удаления настройки.

Форма **show** используется для отображения сервиса или порта на реальном сервере.

3.16. service lvs virtual-address <ip-адрес> real-server <ip-адрес> upper-treshold <число_подключений>

Указание максимального количества подключений к определенному реальному серверу.

Синтаксис

```
set service lvs virtual-address <ip-адрес> real-server <ip-адрес> upper-treshold <число_подключений>
delete service lvs virtual-address <ip-адрес> real-server <ip-адрес> upper-treshold [<число_подключений>]
show service lvs virtual-address <ip-адрес> real-server <ip-адрес> upper-treshold
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   lvs {
      virtual-address ip-адрес {
         real-server ip-адрес {
             upper-treshold число_подключений
         }
      }
   }
}
```

Параметры

virtual-address ip-адрес

IPv4-адрес, указываемый в качестве адреса виртуального сервера.

real-server ip-адрес

IPv4-адрес реального сервера, на который будет выполняться переадресация.

число_подключений

Задает максимальное число подключений к указанному реальному серверу. Диапазон значений u32.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для указания максимального количества подключений к реальному серверу.

Форма **delete** данной команды используется для удаления значения максимального количества подключений.

Форма **show** используется для отображения максимального количества подключений к указанному реальному серверу.

3.17. service lvs virtual-address <ip-адрес> real-server <ip-адрес> weight <вес>

Указание веса для определенного реального сервера.

Синтаксис

```
set service lvs virtual-address <ip-адрес> real-server <ip-адрес> weight
<вес>delete service lvs virtual-address <ip-адрес> real-server <ip-адрес>
weight [<вес>] show service lvs virtual-address <ip-адрес> real-server <ip-
адрес> weight
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   lvs {
      virtual-address ip-адрес {
         real-server ip-адрес {
             weight вес
         }
      }
   }
}
```

Параметры

*virtual-address ip-адрес*IPv4-адрес, указываемый в качестве адреса виртуального сервера.

real-server ip-адрес

IPv4-адрес реального сервера, на который будет выполняться переадресация.

вес

Численное значение веса для реального сервера. Чем больше вес, тем предпочтительнее реальный сервер для переадресации, если это учитывает алгоритм распределения. Диапазон значений u32.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для указания веса для реального сервера.

Форма **delete** данной команды используется для удаления значения веса для реального сервера.

Форма **show** используется для отображения веса на реальном сервере.

3.18. service lvs virtual-address <ip-адрес> scheduler-algo <алгоритм>

Указание алгоритма распределения нагрузки по реальным серверам.

Синтаксис

```
set service lvs virtual-address <ip-адрес> scheduler-algo <алгоритм>
```

```
delete service lvs virtual-address <ip-адрес> scheduler-algo [<алгоритм>]
show service lvs virtual-address <ip-адрес> scheduler-algo
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   lvs {
      virtual-address ip-адрес {
         scheduler-algo алгоритм
      }
   }
}
```

Параметры

virtual-address ip-адрес

IPv4-адрес, указываемый в качестве адреса виртуального сервера.

алгоритм

Алгоритм распределения нагрузки по реальным серверам. Может принимать следующие значения:

- rr: Round-Robin (циклический);
- wrr: Weighted Round-Robin (циклический с учетом весов реальных серверов);
- lc: Least-Connection. Алгоритм с выбором реального сервера с наименьшим количеством подключений;
- wlc: Weighted-Least-Connection. Алгоритм с выбором реального сервера с наименьшим количеством подключений с учетом весов реальных серверов;
- lblc: Locality-Based-Least-Connection. Алгоритм распределения нагрузки с учетом IP-адреса назначения (реального сервера). Применяется в основном для кластеров прозрачных прокси или кэширующих кластерах;
- dh: Destination-Hash. Еще один алгоритм с учетом IP-адреса назначения. Как и lblc позволяет направлять последующие запросы с тем же адресом назначения к одному и тому же реальному серверу;
- sh: Source-Hash. Алгоритм распределения нагрузки с учетом IP-адреса клиента. Может применяться в аналогичных ситуациях с алгоритмами lblc и dh. Запрос от одного и того же клиента будет направляться на один и тот же реальный сервер.

Значение по умолчанию

По умолчанию используется алгоритм rr: Round-Robin (циклический).

Указания по использованию

Форма **set** данной команды используется для указания алгоритма распределения нагрузки по реальным серверам.

Форма **delete** данной команды используется для восстановления значения по умолчанию.

Форма **show** используется для отображения алгоритма распределения нагрузки.

3.19. service lvs virtual-address <ip-адрес> service <сервис>

Указание сервиса или порта виртуального сервера.

Синтаксис

```
set service lvs virtual-address <ip-адрес> service <сервис>
delete service lvs virtual-address <ip-адрес> service [<сервис>]
show service lvs virtual-address <ip-адрес> service
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   lvs {
      virtual-address ip-адрес {
         service сервис
      }
   }
}
```

Параметры

ip-адрес

IPv4-адрес, указываемый в качестве адреса виртуального сервера.

сервис

Имя сервиса или порт, обращения к которому будут переадресовываться на реальные серверы.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** данной команды используется для указания сервиса виртуального сервера.
Форма **delete** данной команды используется для удаления порта виртуального сервера.
Форма **show** используется для отображения порта виртуального сервера.

3.20. service lvs show

Отображение сведений о состоянии сервиса LVS.

Синтаксис

```
service lvs show [ checks | connections | statistics ]
```

Режим ввода команды

Эксплуатационный режим.

Параметры

checks

Показывает информацию о доступности реальных серверов в составе LVS.

connections

Показывает информацию об установленных через сервис LVS соединениях.

statistics

Показывает статистику по сервису LVS, включая в себя информацию по пакетам и объему трафика.

Указания по использованию

Эта команда используется для просмотра сведений о настроенном сервисе LVS.

Без дополнительных аргументов команда выводит сведения о текущих настройках сервиса и количеству подключений.

LVS настраивается с помощью команды `service lvs`.

Примечание. В случае отсутствия сконфигурированных проверок доступности параметр `checks` всегда будет отображать информацию о том, что имеющиеся реальные серверы доступны. Это связано с тем, что команда операционного режима не имеет представления о запущенной конфигурации и лишь выводит информацию, полученную от соответствующей службы. С точки зрения запущенной службы, если проверок доступности не сконфигурировано, все серверы считаются доступными.

Примеры

В примере 2 приведен образец вывода команды `service lvs show` без параметров.

Пример 2 - Вывод команды `service lvs show`

```
admin@edge-lvs:~$ service lvs show
Виртуальный IP:Порт Протокол Алгоритм
  -> Реальный IP:Порт Пересылка Вес Акт.Подкл. Неакт.Подкл.
192.168.1.100:22    UDP,TCP rr
  -> 100.64.0.2:22  Masq    1   1    0
admin@edge-lvs:~$
```

В примере 3 приведен образец вывода команды `service lvs show checks`.

Пример 3 - Вывод команды `service lvs show checks`

```
admin@edge-lvs:~$ service lvs show checks
Виртуальный сервер 192.168.1.100:22:
    Активен: Да
    Реальный сервер 100.64.0.1:22:
        Активен: Да
    Реальный сервер 100.64.0.2:22:
        Активен: Да
admin@edge-lvs:~$
```

В примере 4 представлен вывод команды `service lvs show connections`.

Пример 4 - Вывод команды `service lvs show connections`

```
admin@edge-lvs:~$ service lvs show connections
Отправитель IP:Порт Виртуальный IP:Порт Реальный IP:Порт Состояние
Протокол
192.168.1.254:35706 192.168.1.100:22    100.64.0.2:22   ESTABLISHED TCP
```

В примере 5 представлен вывод команды `service lvs show statistics`.

Пример 5 - Вывод команды `service lvs show statistics`

```
admin@edge-lvs:~$ service lvs show statistics
Кол-во      Входящее     Исходящее    Входящее  Исходящее
 подкл.      пакетов       пакетов        байт       байт
     1           73             50        8497       8487
Подкл./сек. Пакетов/сек. Пакетов/сек. Байт/сек. Байт/сек.
          0            5            3       354        281
```

Межсетевой экран Numa Edge

Руководство администратора

Краткое руководство по настройке

Листов 20

Санкт-Петербург
2021

СОДЕРЖАНИЕ

ИДЕНТИФИКАЦИЯ ДОКУМЕНТА

Название документа	Руководство администратора. Краткое руководство по настройке
Версия документа	1.1.4
Обозначение документа	643.АМБН.00004-01 32 03
Идентификация ОО	Межсетевой экран Numa Edge
Идентификация разработчика	ООО «НумаТех»
Ключевые слова	Межсетевой экран, МЭ, QSG

1. ПОДКЛЮЧЕНИЕ NUMA EDGE

1.1. Настройки по умолчанию

1.1.1. Идентификационные и аутентификационные данные для Numa Edge

Для работы с интерфейсом устройства необходимо пройти процедуру аутентификации с использованием идентификатора учётной записи пользователя и пароля. По умолчанию в системе уже есть одна предварительно определённая учётная запись пользователя со следующими параметрами:

- идентификатор: **admin**
- пароль: **admin**

ПРИМЕЧАНИЕ Пароль для данной учетной записи необходимо изменить сразу же после начала использования системы.

По умолчанию удалённый доступ к Numa Edge разрешён только через управляющий порт Numa Edge. Расположение управляющего порта зависит от модели устройства.

1.1.2. Идентификационные и аутентификационные данные для доступа в БСВВ Numa BIOS

Для доступа к панели управления БСВВ Numa BIOS необходимо пройти процедуру аутентификации с использованием идентификатора учётной записи пользователя и пароля. По умолчанию в Numa BIOS уже есть одна предварительно определённая учётная запись пользователя со следующими параметрами:

- идентификатор: **admin**
- пароль: **Qwe123$**

ПРИМЕЧАНИЯ:

1. Пароль для данной учетной записи необходимо изменить сразу же после начала использования системы.
2. Рекомендуем запомнить/записать в недоступном для злоумышленника месте новые идентификационные и аутентификационные данные. При утрате логина/пароля восстановление этих данных невозможно, для возобновления работоспособности Изделия потребуется полная перепрошивка Изделия в сервисном центре ООО «НумаТех», при этом сохранность информации не гарантируется. Работы по перепрошивке Изделия осуществляются исключительно при наличии действующего сервисного сертификата на это устройство.
3. В случае ввода неправильного пароля более трёх раз административный пользователь будет заблокирован. Для возобновления работоспособности Изделия потребуется полная перепрошивка Изделия в сервисном центре ООО «НумаТех», при этом сохранность информации не гарантируется.
4. Предъявляются следующие требования к паролям:
   а) длина не менее 7 символов;
   б) буквы разного регистра;
   в) наличие цифр;
   г) наличие спецсимволов.
5. После установки нового пароля устройство будет перезагружено.

1.2. Получение доступа для управления

Для управления Numa Edge можно использовать интерфейс командной строки.

Интерфейс командной строки доступен и на управляющем порту, и при подключении через последовательный интерфейс.

1.2.1. Доступ через последовательный порт

При подключении через последовательный порт (RS-232) используются следующие параметры:

- скорость 115200 бит/с;
- без контроля чётности (No parity);
- 8 бит данных (8 data bits);
- 1 стоповый бит (1 stop bit).

1.2.2. Подключение к управляющему порту

Для получения удалённого доступа следует соединить порт Ethernet управляющего компьютера с управляющим портом Numa Edge при помощи кабеля (UTP категории 5), который входит в комплект поставки.

В качестве управляющего компьютера может быть использован любой персональный компьютер или ноутбук, оснащённый 10BASE-T/100BASE-T/1000BASE-T совместимым адаптером Ethernet.

Выбранный для связи с управляющим портом интерфейс Ethernet управляющего компьютера следует настроить на автоматическое получение адреса по DHCP, в результате чего устройством будет выдана конфигурация, достаточная для доступа к интерфейсу управления Numa Edge.

По умолчанию управляющий порт Numa Edge настроен на сеть 192.168.200.0/24 и имеет собственный адрес 192.168.200.1. Этот адрес должен использоваться для доступа к интерфейсам управления.

Для обеспечения безопасной передачи данных по протоколу SSH используется шифрование на основе стандартов ГОСТ Р 34.12-2018, ГОСТ Р 34.13-2018, а также аутентификация на основе стандарта ГОСТ 34.10—2012. По этой причине на управляющем компьютере должен использоваться клиент SSH, поддерживающий указанные криптографические алгоритмы.

1.3. Защита от сбоев при запуске

В Изделии Numa Edge присутствует механизм защиты от сбоев при запуске: соответствующий механизм призван выявить возможные неполадки Изделия на ранних стадиях эксплуатации. При старте Изделия базовая система ввода-вывода (БСВВ, BIOS) выставляет специализированное значение переменной («статус загрузки»), после чего управление передается операционной среде. При этом ожидается, что операционная среда при полностью успешном старте снимет установленное значение. Считается, что если статус был снят, то ПАК загрузился и работал в штатном режиме, иное значение «статуса загрузки», сигнализирует об ошибке загрузки ПАК. Значение рассматриваемой переменной (статуса загрузки) анализируется базовой системой ввода-вывода при каждом старте, и если значение сигнализирует об ошибке в процессе предыдущей загрузки Изделия - процесс текущей загрузки Изделия будет прерван, а на консольный порт Изделия будет выведено соответствующее сообщение об ошибке.

Перечень возможных сообщений БСВВ:

- «Ошибка контроля целостности Numa Edge».
- «Ошибка конфигурирования сервисов Numa Edge».
- «Ошибка запуска управляющего ПО: превышен лимит неудачных попыток запуска Numa Edge».

В случае возникновения соответствующего сообщения - необходимо изучить, что могло служить его причиной, а также перейти в панель управления БСВВ для вызова штатной загрузки Изделия.

ПРЕДУПРЕЖДЕНИЕ Если в процессе загрузки Изделия Numa Edge произойдет отключение электропитания, то значение соответствующего параметра («статуса загрузки») может быть не сброшено в соответствующее штатному режиму работы. Что в свою очередь вызовет срабатывание описываемого механизма защиты от сбоев. В целях предупреждения такого поведения рекомендуется подключать Изделие Numa Edge к сети электропитания через источники бесперебойного питания.

2. ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС

2.1. Интерфейс командной строки

2.1.1. Режимы команд

Интерфейс командной строки Numa Edge может находиться в двух режимах работы — эксплуатационном и настроечном:

- в эксплуатационном режиме обеспечивается доступ к командам отображения и очистки текущего состояния устройства, отображения конфигурации, включения или выключения отладки, настройки параметров терминалов, сохранения и загрузки состояния, а также перезапуска устройства;
- в настроечном режиме обеспечивается доступ к командам создания, изменения и удаления элементов конфигурации, а также к командам переходов по иерархии параметров.

По умолчанию, при входе в систему интерфейс находится в эксплуатационном режиме. Для перехода из эксплуатационного режима в режим настройки используется команда **configure**.

Для возврата из режима настройки в эксплуатационный режим используется команда **exit**. Переход в эксплуатационный режим при не зафиксированных изменениях в конфигурации не допускается, о чём устройство выдаёт соответствующее предупреждение. В этом случае, изменения необходимо либо применить с помощью команды **commit**, либо отменить с помощью команды discard (или выходить из режима настройки с помощью команды **exit discard**).

При выполнении команды **exit** в эксплуатационном режиме происходит выход из системы.

Когда устройство ожидает ввода команд, оно показывает соответствующее приглашение, которое также информирует пользователя о том, в каком режиме он работает с командной строкой, от имени какой учетной записи он работает и каково имя системы:

`admin@edge:-$`	Учётная запись: admin Имя системы: edge Режим интерфейса: эксплуатационный (символ «$»)
`[edit policy]` `admin@gate4#`	Учётная запись: admin Имя системы: gate4 Режим интерфейса: настроечный (символ «#») Ветвь конфигурации: policy

2.1.2. Автодополнение команд

В интерфейсе командной строки имеется функция автодополнения вводимых команд по первым введённым символам. Она задействуется клавиатурными комбинациями, описанными в таблице 1.

Таблица 1 – Клавиши автодополнения

Нажатые клавиши	**Результат**
<Tab>	Автодополнение команды: • если введённые символы можно дополнить однозначно, до единственной команды, то это и происходит; • если возможен более чем один вариант авто- дополнения, то система отображает список возможных последующих команд. При повторном нажатии клавиши <Tab> отображается справка интерфейса командной строки для списка возможных последующих команд.
?	При нажатии на клавишу с вопросительным знаком («?») также выполняется автодополнение команды. Для «обычного» ввода символа вопросительного знака, следует сначала нажать <Ctrl>+v, потом вопросительный знак.

3. КОНФИГУРАЦИЯ

3.1. Общие сведения по конфигурации

3.1.1. О возможности одновременного редактирования конфигурации

ПРЕДУПРЕЖДЕНИЕ Система конфигурирования Numa Edge не обеспечивает возможности одновременного редактирования конфигурации. К таким ситуациям относятся:

- одновременное редактирование конфигурации несколькими пользователями;
- одновременное редактирование конфигурации различными способами подключения (доступ к интерфейсу командной строки через последовательный порт, подключение по SSH, использование web-интерфейса).

В случаях, когда вероятна ситуация одновременной работы с конфигурацией, в первую очередь перед внесением изменений следует воспользоваться командой конфигурационного режима **show**. Если вы видите, что большая часть конфигурации устройства помечена на удаление, значит конфигурация была изменена в другой сессии. В таком случае предварительно следует выполнить команду **discard**.

3.1.2. Иерархия дерева конфигурации

Конфигурация устройства имеет древовидное строение и разделяется логически на узлы и атрибуты конфигурации. Атрибут конфигурации имеет вид атрибут значение, как в приведённом ниже примере:

```
cipher aes256-ctr
```

У узла конфигурации всегда есть закрытая пара фигурных скобок, содержимое которой может быть пусто, как в следующем примере:

```
service {
   https {
   }
}
```

или непусто, как в следующем примере:

```
ssh {
    address 192.168.1.1
}
```

3.1.3. Добавление параметров к конфигурации или изменение конфигурации

Добавление нового параметра производится в режиме настройки через создание атрибутов и узлов конфигурации командой **set**. Изменение существующего параметра выполняется тоже в режиме настройки с помощью команды **set**, как в приведённом ниже примере:

```
[edit]
admin@edge# set interfaces ethernet eth2 address 192.168.1.100/24
```

Затем для просмотра изменений можно использовать команду **show**:

```
[edit]
admin@edge# show interfaces ethernet eth2
+address  192.168.1.100/24
```

Обратите внимание на знак «+» перед новым оператором. Он показывает, что оператор был добавлен к конфигурации, но изменение ещё не зафиксировано. Изменение не вступит в силу до тех пор, пока конфигурация не будет зафиксирована с помощью команды **commit**.

Конфигурацию можно изменять, начиная с корня дерева конфигурации или использовать команду **edit** для перемещения к той ветви дерева, в которой надо выполнить изменения, а также команды **up** и **top** для возврата на верхние уровни.

При первой загрузке системы дерево конфигурации практически пусто, за исключением нескольких автоматически настроенных узлов. Вся функциональность системы настраивается через создание и изменение узлов и атрибутов конфигурации. Когда создаётся новый узел, для всех его атрибутов применяются значения по умолчанию.

3.1.4. Удаление параметров

Для удаления атрибута или целого узла в настройке служит команда **delete**, как в приведённом ниже примере:

```
[edit]
admin@edge# delete interfaces ethernet eth2 address 192.168.1.100/24
```

Затем для просмотра изменений можно использовать команду **show**:

```
[edit]
admin@edge# show interfaces ethernet eth2
-address 192.168.1.100/24
```

Обратите внимание на знак «-» перед удалённым атрибутом. Он показывает, что атрибут был удалён из конфигурации, но изменение еще не зафиксировано. Изменение не вступит в силу до тех пор, пока конфигурация не будет зафиксирована с помощью команды **commit**.

Некоторые узлы и атрибуты конфигурации являются обязательными, среди них есть такие, которые нельзя удалить, а есть имеющие значения по умолчанию, при удалении которых для них будет восстановлено это значение.

3.1.5. Фиксация изменений конфигурации

Изменения в конфигурации вступают в силу только после их фиксации командой **commit**:

```
[edit]
admin@edge# commit
```

При просмотре конфигурации имеющиеся незафиксированные изменения помечаются знаком «+» (в случае добавления/правки) или «-» (в случае удаления). При фиксации изменений знаки удаляются, как в приведённом ниже примере:

```
[edit]
admin@edge# show interfaces ethernet eth2
-address 192.168.1.100/24
[edit]
admin@edge# commit
[edit]
admin@edge# show interfaces ethernet eth2
[edit]
admin@edge#
```

Изменения фиксируются в текущей (активной) конфигурации. Для того чтобы полученная конфигурация использовалась после перезагрузки устройства она должна быть сохранена в файл командой **save**, см. раздел «Сохранение конфигурации в файл».

3.1.6. Отмена изменений в конфигурации

Выйти из режима настройки при наличии незафиксированных изменений невозможно: необходимо либо фиксировать изменения, либо отказаться от них. Если фиксировать изменения не нужно, можно отменить их с помощью команды **exit discard**:

```
[edit]
admin@edge# exit
Cannot exit: configuration modified.
Use 'exit discard' to discard the changes and exit.
[edit]
admin@edge# exit discard
admin@edge01:~$
```

3.1.7. Сохранение конфигурации в файл

Действующую в данный момент конфигурацию можно сохранить в файл при помощи команды **save** в режиме настройки. По умолчанию, конфигурация сохраняется в файл config.boot в стандартном каталоге конфигурации, которым является /etc/config:

```
[edit]
admin@edge# save
Запись конфигурации в '/etc/config/config.boot'...
Готово
```

При включении питания устройство загружает конфигурацию именно из файла /etc/config/config.boot, поэтому после успешной настройки всех необходимых сервисов важно сохранить текущую конфигурацию в этот файл.

Можно сохранить конфигурацию под другим именем, указав другое имя файла:

```
[edit]
admin@edge# save testconfig
Запись конфигурации в  '/etc/config/testconfig'...
Готово
```

Для сохранения файла конфигурации можно указать и другой каталог, отличный от стандартного /etc/config. Сохранять можно на жесткий диск, карту CF или USB-накопитель, включив точку монтирования носителя в путь. Также поддерживается сохранение файла на сервера FTP, TFTP. Перед тем, как конфигурацию можно будет сохранить на флэш-накопитель, последний следует смонтировать командой **flash mount** в эксплуатационном режиме.

Обратите внимание, что команда **save** записывает только актуальную конфигурацию.

3.1.8. Загрузка конфигурации

Для загрузки ранее сохранённой конфигурации используется команда **load** в режиме настройки. По умолчанию система считывает файл из стандартного каталога конфигурации — /etc/config:

```
[edit]
admin@edge# load testconfig
Loading config file /etc/config/testconfig...
```

```
Done
```

Загруженная конфигурация автоматически применяется и становится активной конфигурацией.

Для загрузки файла конфигурации можно указать и другой каталог, отличный от стандартного /etc/config. Загружать конфигурацию можно с жесткого диска карт CF или USB-накопителей, включив точку монтирования носителя в путь. Также поддерживается загрузка конфигурации с серверов FTP, TFTP или HTTP.

В таблице 2 приведены поддерживаемые устройством пути для сохранения или загрузки файла конфигурации:

Таблица 2 – Способы указания местоположения файла конфигурации

Местоположение	**Способ указания**
Абсолютный путь	Используется стандартный способ указания файла в UNIX
Относительный путь	Указывается имя файла относительно стандартного каталога /etc/config.
Сервер TFTP	Используется следующий синтаксис для имени файла: tftp://ip-адрес/файл_конфигурации, где ip-адрес это IP-адрес сервера TFTP, а файл_конфигурации это файл конфигурации, включая путь относительно корневого каталога TFTP.
Сервер FTP	Используется следующий синтаксис для имени файла: ftp://ip-адрес/файл_конфигурации, где ip-адрес — это IP-адрес сервера FTP, а файл_конфигурации — это файл конфигурации, включая путь. При использовании FTP будет выдан запрос на ввод имени учётной записи на сервере FTP и её пароля.
Сервер HTTP (только для загрузки конфигурации)	Используется следующий синтаксис для имени файла: http://ip-адрес/файл_конфигурации, где ip-адрес это IP-адрес сервера HTTP, а файл_конфигурации это файл конфигурации, включая путь.

3.2. Пример. Базовая конфигурация

В этом разделе приведён пример начальной настройки системы. Для доступа к интерфейсу командной строки используется протокол SSH. Работа ведётся от имени учетной записи, определённой по умолчанию: идентификатор пользователя — admin, пароль — admin.

3.2.1. Переход в режим настройки

После входа в систему мы оказываемся в эксплуатационном режиме, являющимся режимом по умолчанию:

```
Last login: Mon Sep  7 13:48:00 MSK 2020 from  192.168.200.100
admin@edge:-$
```

Для настройки системы необходимо перейти в режим настройки:

```
admin@edge:-$ configure
[edit]
admin@edge#
```

3.2.2. Установка имени системы

По умолчанию системе присвоено имя edge. При необходимости это значение можно изменить:

```
[edit]
admin@edge# set system host-name gate
[edit]
```

```
admin@edge# commit
```

Вид приглашения, соответствующий новому имени системы, появится при следующем входе в систему.

3.2.3. Установка имени домена

В дополнение к изменению имени системы, может потребоваться изменить имя домена:

```
[edit]
admin@edge# set system dns domain-name numatech.ru
[edit]
admin@edge# commit
```

3.2.4. Изменение пароля

По умолчанию в системе есть одна предварительно определённая учётная запись пользователя:

- идентификатор пользователя: **admin;**
- пароль по умолчанию: **admin.**

Пароль для данной учётной записи необходимо изменить сразу же после начала использования системы:

```
[edit]
admin@edge# set system login user admin authentication plaintext-password
'bt12plo%14P'
[edit]
admin@edge# commit
```

3.2.5. Настройка интерфейсов

Тип и номер изменяемого интерфейса зависят от используемого устройства и топологии сети. Однако, практически при любой топологии сети требуется настройка по крайней мере одного интерфейса Ethernet. В этом примере приведена настройка интерфейса eth1 в качестве интерфейса, к которому подключён внешний сегмент сети:

```
[edit]
admin@edge# set interfaces ethernet eth1 address 203.0.113.10/24
[edit]
admin@edge# commit
```

В том случае, когда провайдер предоставляет сетевые настройки по протоколу DHCP, следует использовать команду **set interfaces ethernet eth1 address dhcp**.

Для просмотра текущей настройки используется команда **show**:

```
[edit]
admin@edge# show interfaces ethernet
eth1 {
    address 203.0.113.10/24
}
```

3.2.6. Настройка маршрута по умолчанию

Получателем трафика, для которого Numa Edge не может определить маршрут исходя из собственных таблиц маршрутизации, является другое внешнее устройство, называемое

маршрутизатором по умолчанию (а путь отправки такого трафика называется маршрутом по умолчанию). Адрес маршрутизатора по умолчанию указывается следующим образом:

```
[edit]
admin@edge# set system gateway-address 203.0.113.100
[edit]
admin@edge# commit
```

3.3. Пример. Интернет-шлюз

Рассматриваемая в этом примере конфигурация предполагает следующее:

- настройка маршрутизации сетевого трафика между локальной сетью (LAN) и интернетом;
- возможность получения доступа к Numa Edge по протоколу SSH из внутренней сети;
- назначение адресов устройствам во внутренней локальной сети динамически, по протоколу DHCP;
- использование ретрансляции DNS для устройств во внутренней локальной сети;
- использование NAT для преобразования внутренних адресов в один внешний адрес;
- настройка межсетевого экрана для предотвращения доступа к системе из внешнего сегмента сети (интернета).

В данном примере приведена настройка двух интерфейсов Ethernet, к одному из которых (eth1) подключён внешний сегмент сети (WAN), а к другому (eth2) подключён локальный сегмент сети (LAN), как показано на рисунке 1.

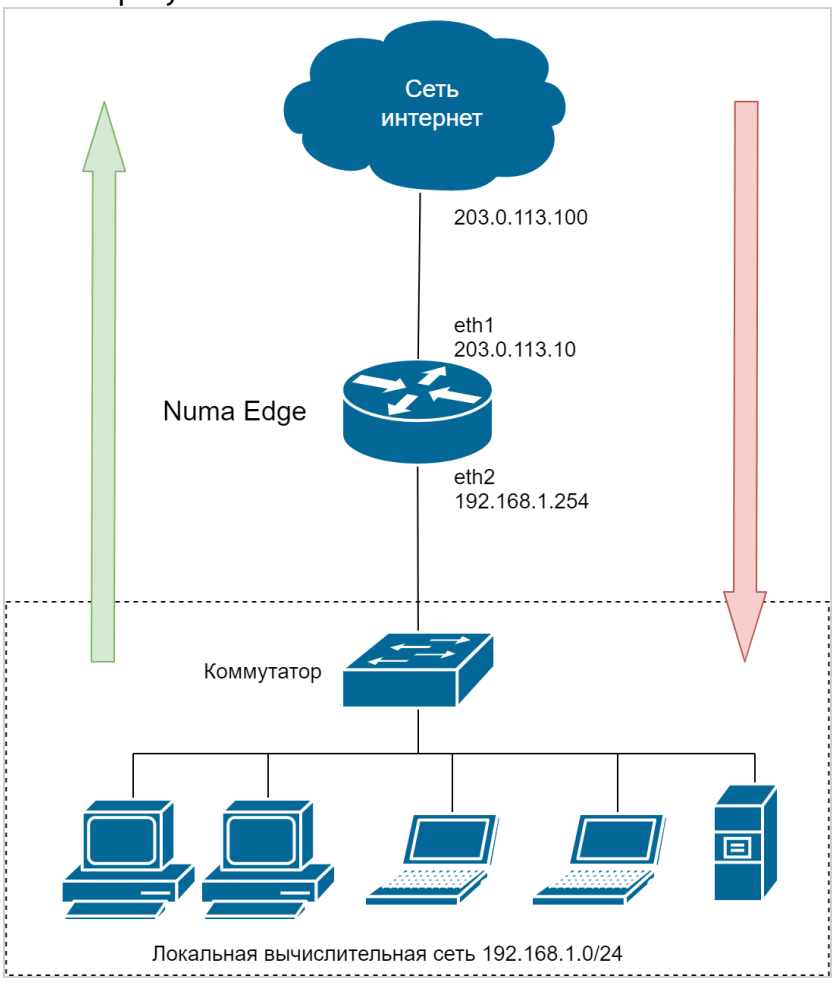


Рисунок 1 – Интернет-шлюз

В этом примере также предполагается, что уже выполнена настройка из предыдущего примера.

3.3.1. Настройка интерфейсов

В предыдущем примере был настроен внешний интерфейс eth1. Для того, чтобы Numa Edge функционировал в качестве интернет-шлюза, в системе необходимо настроить ещё один интерфейс, к которому будет подключён локальный сегмент сети (LAN). В нашем случае используется интерфейс eth2:

```
[edit]
admin@edge# set interfaces ethernet eth2 address 192.168.1.254/24
[edit]
admin@edge# commit
```

Для просмотра текущей настройки используется команда **show**:

```
[edit]
admin@edge# show interfaces ethernet
    eth1 {
        address 203.0.113.10/24
    }
    eth2 {
        address 192.168.1.254/24
    }
```

3.3.2. Включение доступа по протоколу SSH

По умолчанию доступ к Numa Edge по протоколу SSH разрешён только на управляющем интерфейсе. Доступ из локальной сети включается следующей командой:

```
[edit]
admin@edge# set service ssh address 192.168.1.254
[edit]
admin@edge# commit
```

Для просмотра текущей настройки используется команда **show**:

```
[edit]
admin@edge# show service ssh
   address 192.168.1.254 {
   }
   cipher kuznechik-ofb
   hmac hmac-stribog-256
   hmac hmac-stribog-512
   key-exchange-algo ecdh-gost2012-256-cpa
   client-alive-timeout 1800
   disable-password-authentication false
```

3.3.3. Настройка сервера DHCP

Протокол динамической настройки системы (Dynamic Host Configuration Protocol, DHCP) обеспечивает динамическое назначение IP-адресов и других сведений о настройке системам указанного сегмента сети. В нашем примере сервер DHCP обеспечивает динамическое назначение IP-адресов компьютерам в локальной сети (LAN).

В настройке сервера DHCP необходимо определить перечень (блок/пул) адресов, которые будут выдаваться клиентам в локальной сети (192.168.1.100—192.168.1.199). В качестве маршрутизатора по умолчанию и сервера доменных имен будет указываться адрес внутреннего интерфейса (eth2) Numa Edge:

```
[edit]
admin@edge# set service dhcp-server subnet 192.168.1.0/24 start 192.168.1.100
stop 192.168.1.199
[edit]
admin@edge# set service dhcp-server subnet 192.168.1.0/24 default-router
192.168.1.254
[edit]
admin@edge# set service dhcp-server subnet 192.168.1.0/24 dns-server
192.168.1.254
[edit]
admin@edge# commit
```

Для просмотра текущей настройки используется команда **show:**

```
[edit]
admin@edge# show service dhcp-server
   subnet 192.168.1.0/24 {
        default-router 192.168.1.254
        start 192.168.1.100 {
            stop 192.168.1.199
        }
   }
```

3.3.4. Настройка DNS

3.3.4.1. Системный сервер DNS

Настраиваемый системный сервер DNS будет использоваться самим Numa Edge и всеми его сервисами для разрешения имён. Обычно указывается предоставленный провайдером сервер DNS. В отсутствие настройки конкретного используемого сервера DNS будут использоваться сервера, получаемые с помощью протокола DHCP, либо полученные через туннели PPPoE, PPTP, OpenVPN и т.п. Статическая настройка использования конкретного сервера выполняется следующим образом:

```
[edit]
admin@edge# set system dns name-server 203.0.113.100
[edit]
admin@edge# commit
```

Для просмотра текущей настройки используется команда **show**:

```
[edit]
admin@edge# show system dns
   domain-name numatech.ru
   name-server 203.0.113.100 {
   }
```

3.3.4.2. Сервис ретрансляции DNS

Сервис ретрансляции DNS позволяет клиентам локальной сети использовать Numa Edge для разрешения имён посредством протокола DNS. По умолчанию, сам сервис использует доступные системные сервера DNS, а настройка доступа требует указания интерфейса. В данном примере необходимо указать внутренний интерфейс (eth2):

```
[edit]
admin@edge# set service dns forwarding listen-on address 192.168.1.254
[edit]
admin@edge# commit
```

Для просмотра текущей настройки используется команда **show**:

```
[edit]
admin@edge# show service dns forwarding
   listen-on {
       address 192.168.1.254
   }
```

3.3.5. Настройка NAT

Интернет-шлюз должен отправлять исходящий сетевой трафик из локальной сети через внешний интерфейс и заменять внутренние адреса на внешний общедоступный адрес. Для этого необходимо определить правило NAT.

Определим правило, обеспечивающее прохождение трафика из внутренней подсети 192.168.1.0/24 в интернет через интерфейс eth1 и заменяющее внутренние адреса на внешний адрес интерфейса eth1:

```
[edit]
admin@edge# set service nat ipv4 rule 1 source address 192.168.1.0/24
[edit]
admin@edge# set service nat ipv4 rule 1 outbound-interface eth1
[edit]
admin@edge# set service nat ipv4 rule 1 type masquerade
[edit]
admin@edge# commit
```

Для просмотра текущей настройки используется команда **show**:

```
[edit]
admin@edge# show service nat ipv4
   rule 1 {
       outbound-interface eth1
```

```
        source {
            address 192.168.1.0/24
        }
        type masquerade
    }
```

3.3.6. Настройка межсетевого экрана (МЭ)

При настройках по умолчанию Numa Edge никак не ограничивает прохождение сетевого трафика. Передача трафика через интерфейс разрешена до тех пор, пока к интерфейсу не будет применено правило МЭ. В данном примере интернет-шлюз должен разрешать доступ к интернету устройствам из локальной сети и собственным службам, но необходимо блокировать трафик, инициированный источниками из внешнего сегмента сети.

В общем случае, для настройки правил МЭ на интерфейсе необходимо сделать следующее:

- определить поименованные наборы правил МЭ (т.н. экземпляры МЭ), каждый из которых может содержать одно или более правил;
- применить необходимые экземпляры МЭ к интерфейсу. Экземпляр МЭ может фильтровать пакеты одного из следующих направлений:
  - **in** (входящий). Если применить экземпляр с использованием ключевого слова **in,** то межсетевой экран будет фильтровать пакеты, входящие в интерфейс и транзитно проходящие через устройство;
  - **out** (исходящий). Если применить экземпляр с использованием ключевого слова **out,** то межсетевой экран будет фильтровать транзитные пакеты, проходящие через устройство, и покидающие её через указанный интерфейс;
  - **local** (локальный). Если применить экземпляр с использованием ключевого слова **local,** то межсетевой фильтр будет фильтровать пакеты, предназначенные самому устройству (не транзитные).

При этом для одного направления трафика может быть применён только один экземпляр МЭ.

3.3.6.1. Определение экземпляра МЭ

Создание правила для пропуска в локальный сегмент сети только ответного трафика, порождённого исходящим трафиком этого сегмента (т.е. установленными из LAN наружу соединениями и связанным с ними трафиком):

```
[edit]
admin@edge# set filter ALLOW_ESTABLISHED
[edit]
admin@edge# set filter ALLOW_ESTABLISHED rule 10
[edit]
admin@edge# set filter ALLOW_ESTABLISHED rule 10 state established enable
[edit]
admin@edge# set filter ALLOW_ESTABLISHED rule 10 state related enable
[edit]
admin@edge# set policy firewall ALLOW_ESTABLISHED
[edit]
admin@edge# set policy firewall ALLOW_ESTABLISHED rule 10 action accept
```

```
[edit]
admin@edge# set policy firewall ALLOW_ESTABLISHED rule 10 match filter
ALLOW_ESTABLISHED
[edit]
admin@edge# commit
```

3.3.6.2. Применение экземпляра МЭ к интерфейсу

Применение набора правил ALLOW_ESTABLISHED к сетевому трафику, приходящему на интерфейс:

```
[edit]
admin@edge# set interfaces ethernet eth1 policy in firewall ALLOW_ESTABLISHED
[edit]
admin@edge# set interfaces ethernet eth1 policy local firewall
ALLOW_ESTABLISHED
```

Если в разделе «Настройка интерфейсов» использовалась настройка внешнего интерфейса по DHCP, применение МЭ к направлению local сделает невозможной конфигурацию интерфейса по DHCP, следует либо не применять соответствующую настройку, либо добавить разрешительные правила для протокола DHCP в МЭ.

Для просмотра текущей настройки используется команда **show**:

```
[edit]
admin@edge# show policy firewall
   ALLOW_ESTABLISHED {
       rule 10 {
           action accept
           match {
               filter ALLOW_ESTABLISHED
           }
       }
   }
[edit]
admin@edge# show filter
   ALLOW_ESTABLISHED {
       rule 10 {
           state {
               established enable
               related enable
           }
       }
   }
[edit]
admin@edge#
```

Просмотр параметров интерфейса:

```
admin@edge# show interfaces
   ethernet eth1 {
       address 203.0.113.21/24
       policy {
           in {
               firewall ALLOW_ESTABLISHED
           }
           local {
               firewall ALLOW_ESTABLISHED
           }
       }
   }
   ethernet eth2 {
       address 192.168.1.254/24
   }
```

4. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для создания заявок и переписки с сервисной службой существует портал, доступный по адресу https://support.numatech.ru/. Взаимодействовать с сервисной службой можно также через почту, заявки автоматически создаются для писем, направленных на адрес support@numatech.ru.

Для ускорения обработки заявок, рекомендуется сопровождать их выводом команды эксплуатационного режима **show tech-support**. Сохранить вывод **show tech-support** на флэш-накопитель вы можете следующим образом:

Подключите флэш-накопитель к устройству (накопитель должен быть форматирован в файловую систему FAT или FAT32);

Выполните следующие эксплуатационные команды:

```
admin@edge:-$flash mount
admin@edge:-$show tech-support save /media/hdd/tech
admin@edge:-$flash umount
```

Извлеките флэш-накопитель из устройства.

В корневом каталоге будет находиться файл с именем tech.[имя_устройства].tech-support.[текущая_дата].gz, который и необходимо отправить специалистам сервисной службы.

Межсетевой экран Numa Edge

Руководство администратора

Использование FTP proxy

Листов 25

Санкт-Петербург
2022

СОДЕРЖАНИЕ

ИДЕНТИФИКАЦИЯ ДОКУМЕНТА

Название документа	Руководство администратора. Использование FTP proxy
Версия документа	1.2.1
Обозначение документа	643.АМБН.00004-01 32 05
Идентификация ОО	Межсетевой экран Numa Edge
Идентификация разработчика	ООО «НумаТех»
Ключевые слова	Межсетевой экран, МЭ, ftpproxy

ВВЕДЕНИЕ

Протокол FTP (File Transfer Protocol) является одним из старейших прикладных протоколов и предназначен для передачи файлов между сервером и клиентом. Данный протокол для работы поверх IP был описан в RFC 765 и RFC 959 и в дальнейшем дополнялся различными стандартами. Для фильтрации данного протокола в Numa Edge присутствует функционал ftpproxy, который позволяет осуществлять фильтрацию команд прикладного уровня протокола. В данном документе описано использование функционала ftpproxy.

1. ОПИСАНИЕ РАБОТЫ ПРОТОКОЛА FTP

Типичным сценарием использования протокола FTP является установления соединение клиента с сервером с последующей загрузкой файлов с сервера либо на сервер. Установления соединения может осуществляться после ввода клиентом идентификационных данных либо без них (на сервере может быть разрешен анонимный режим работы). Протокол FTP использует два параллельных TCP-соединения:

- управляющее соединение, через которое передаются команды протокола и получаются ответы;
- соединение данных, через которое передаются файлы, где для каждого нового передаваемого файла открывается новое соединение.

Для управляющего соединения используется порт 21/TCP, к которому подключается клиент. Это соединение, в отличие от соединения данных, активно на протяжении работы с FTP-сервером и передачи информации.

Используемый порт для соединения данных изменяется в зависимости от режима работы FTP-сервера:

- в активном режиме – клиент передает серверу номер порта, который он открывает для подключения сервера. Исходящий порт сервера 20/TCP;
- в пассивном режиме – в этом случае сервер сам назначает порт для соединения данных из предварительного настроенного диапазона (по умолчанию 1024-65535). Данный режим, после изменения диапазона портов пассивного режима, принято использовать при прохождении FTP-соединения через NAT.

2. ВОЗМОЖНОСТИ ФИЛЬТРАЦИИ ПРОТОКОЛА FTP С ИСПОЛЬЗОВАНИЕМ FTP PROXY

FTP-прокси, как и любой другой прокси-сервер, использует промежуточное устройство посредника для сокрытия реального IP адреса. Применимо к FTP-прокси, возможно расположение FTP-сервера внутри защищенного периметра и настройка на Numa Edge службы ftpproxy для сокрытия реального IP-адреса сервера. Другой особенностью данной службы является разбор передаваемых сообщений внутри управляющего соединения, с последующим принятием решения о разрешении или запрете их передачи в зависимости от IP-адресов отправителя и получателя, а также имени пользователя.

Правила фильтрации разделены на две группы:

- **auth-rules:** правила аутентификации, которые выполняются на этапе подключения к прокси-серверу и регламентируют возможность данного подключения;
- **command-rules:** правила команд, которые работают только после успешной аутентификации и регламентируют возможность выполнения команд.

Функционал Numa Edge позволяет фильтровать следующие команды протокола:

- APPE – добавить новый файл;
- CDUP – перейти в родительский каталог;
- CWD – перейти в директорию;
- DELE – удалить файл;
- LIST – получить содержимое каталога;
- MDTM – вернуть время последнего изменения указанного файла;
- MKD – создать директорию;
- NLST – вернуть список имен файлов в указанном каталоге;
- RETR – скачать файл;
- RMD – удалить директорию;
- RNFR – выбрать файл для переименования;
- RNTO – переименовать файл;
- SIZE – вернуть размер файла;
- STAT – вернуть информацию о состоянии сервера, включая состояние текущего соединения;
- STOR – загрузить файл;
- STOU – хранить файл уникальным образом;
- XCUP – перейти к родительскому элементу текущего рабочего каталога;
- XCWD – перейти в директорию;
- XMKD – создать директорию;
- XRMD – удалить директорию.

Обратите внимание, что некоторые команды могут повторять смысл друг друга. Это объясняется различными стандартами RFC, в которых данные команды были описаны.

Примечание. Поддерживается работа (фильтрация) только для 1 FTP-сервера, на который служба ftpproxy перенаправляет соединения. В случае использования парольной аутентификации, имя пользователя и пароль передаются в открытом виде как при установлении соединения от клиента к ftpproxy на Numa Edge, так и от Numa Edge к FTP-серверу. Разбор соединений, зашифрованных TLS (FTPS) службой ftpproxy, не поддерживается.

3. ПРИМЕР НАСТРОЙКИ FTP PROXY

3.1. Настройка правил FTP proxy

В качестве примера настройки службы ftpproxy рассмотрим настройку ограничения, когда определенному пользователю запрещается удалять каталоги и файлы, но при этом разрешается их загружать и скачивать. Пусть существует следующая схема сети, представленная на рисунке 1:

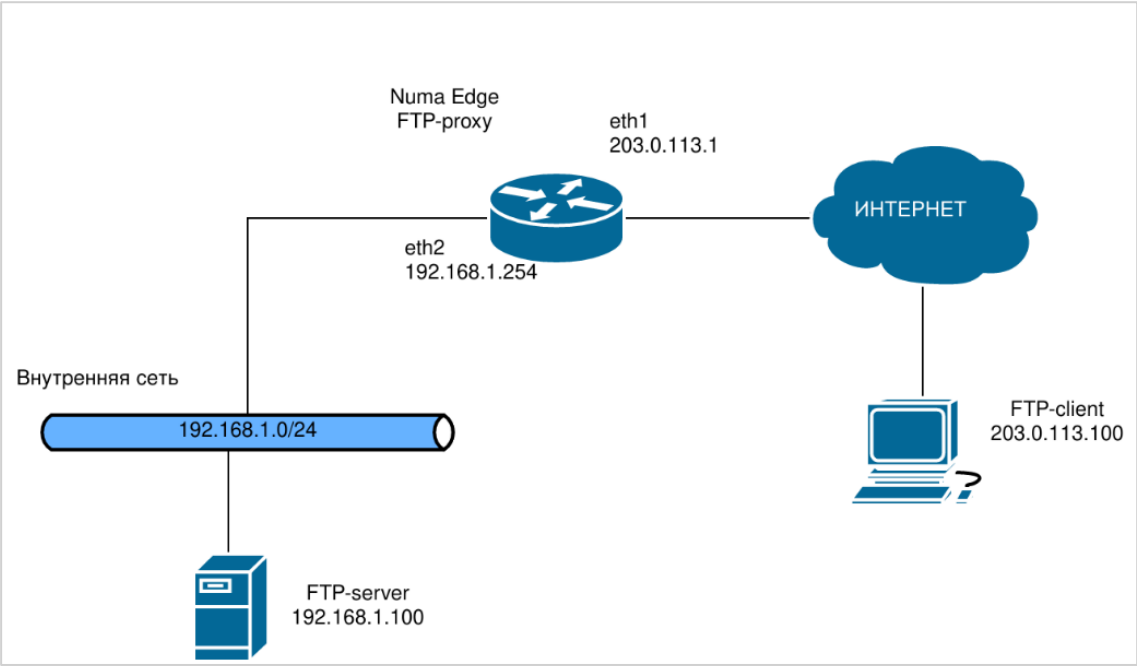


Рисунок 1 – Схема сети с FTP-сервером

В данной схеме Numa Edge выступает в роли FTP-прокси-сервера, и перенаправляет сообщения протокола FTP между клиентом и сервером. Настройка FTP-server и FTP-client в данном примере не рассматривается. В этом примере FTP-server находится во внутренней сети 192.168.1.0/24, а клиенты подключаются из внешней сети Интернет. На Numa Edge настроен адрес из внешней сети на интерфейсе eth1 – 203.0.113.1/24.

Примечание. В этом примере подразумевается, что внутренняя сеть находится за NAT, но поскольку ftpproxy будет настроен на прослушивание адреса из внешней сети 203.0.113.1, то настройка проброса портов для FTP-сервера не потребуется.

Для ограничения возможности удаления файлов и каталогов пользователю ftpuser выполните действия, описанные в примере 1.

Пример 1 – Настройка ftpproxy

Действие	**Команда**
Настройка адреса, на котором ftpproxy будет ожидать соединения. По умолчанию используется порт 21/TCP	`[edit]` `admin@edge# set service ftpproxy internal address '203.0.113.1'`
Настройка адреса FTP-сервера, на который ftpproxy будет перенаправлять соединения	`[edit]` `admin@edge# set service ftpproxy remote-server '192.168.1.100'`
Настройка действия по умолчанию, которое безусловно разрешает все команды для любых пользователей с любых IP-адресов	`[edit]` `admin@edge# set service ftpproxy default-action 'permit'`

Действие	**Команда**
Настройка правила 10, ограничивающее удаление каталогов для пользователя ftpuser	[edit] admin@edge# set service ftpproxy command-rules 10 command 'RMD' [edit] admin@edge# set service ftpproxy command-rules 10 user 'ftpuser' [edit] admin@edge# set service ftpproxy command-rules 10 action 'deny'
Настройка правила 20, ограничивающее удаление файлов для пользователя ftpuser	[edit] admin@edge# set service ftpproxy command-rules 20 command 'DELE' [edit] admin@edge# set service ftpproxy command-rules 20 user 'ftpuser' [edit] admin@edge# set service ftpproxy command-rules 20 action 'deny'
Настройка правила 30, ограничивающее удаление каталогов альтернативной командой FTP для пользователя ftpuser	[edit] admin@edge# set service ftpproxy command-rules 30 command 'XRMD' [edit] admin@edge# set service ftpproxy command-rules 30 user 'ftpuser' [edit] admin@edge# set service ftpproxy command-rules 30 action deny
Применение изменений	[edit] admin@edge# commit

Просмотр полученной конфигурации	[edit]
	admin@edge# show service ftpproxy
	command-rules 10 {
	action deny
	command RMD
	user ftpuser
	}
	command-rules 20 {
	action deny
	command DELE
	user ftpuser
	}
	command-rules 30 {
	action deny
	command XRMD
	user ftpuser
	}
	default-action permit
	internal {
	address 203.0.113.1
	}
	remote-server 192.168.1.100

3.2. Запрет доступа к FTP-серверу для определенного пользователя

Предположим, что необходимо запретить определенному пользователю доступ на FTP-сервер. Для этого необходимо создать запрещающее правило auth-rule, в котором будет указано имя данного пользователя. В следующем примере описано как произвести данную настройку.

Пример 2 – Запрет доступа на FTP-сервер определенному пользователю

Действие	**Команда**
Создание правила доступа, в котором указывает имя пользователя **baduser**	`[edit]` `admin@edge# set service ftpproxy auth-rules 10 user baduser`
Запрет доступа к FTP-серверу для данного пользователя	`[edit]` `admin@edge# set service ftpproxy auth-rules 10 action deny`
Применение изменений	`[edit]` `admin@edge# commit`

Просмотр получившейся конфигурации службы ftpproxy	`[edit]`
	`admin@edge-no-dm# show service ftpproxy`
	`  auth-rules 10 {`
	`  action deny`
	`  user baduser`
	`  }`
	`  command-rules 10 {`
	`  action deny`
	`  command RMD`
	`  user ftpuser`
	`  }`
	`  command-rules 20 {`
	`  action deny`
	`  command DELE`
	`  user ftpuser`
	`  }`
	`  command-rules 30 {`
	`  action deny`
	`  command XRMD`
	`  user ftpuser`
	`  }`
	`  default-action permit`
	`  internal {`
	`  address 203.0.113.1`
	`  }`
	`  remote-server 192.168.1.100`

3.3. Настройка правил МЭ для разрешения только FTP-трафика

В качестве следующего примера будет произведена настройка правил межсетевого экранирования на Numa Edge. Поскольку служба ftpproxy работает на самом Numa Edge, правила будут применяться для входящего локального трафика (направление local) для внешнего интерфейса, к которому подключаются клиенты (eth2 согласно схеме на рисунке 1). Команды, приведенные в данном примере, ограничивают весь трафик, кроме явно разрешенного. Для этого будет создано правило фильтрации трафика, которое будет добавлено в политику межсетевого экранирования. В случае если в реальном использовании у вас уже существует политика межсетевого экранирование, вы можете добавить в нее новое правило по аналогии с представленным примером.

Для разрешения входящих соединений только для FTP-трафика выполните следующие действия:

Пример 3 – Настройка политик межсетевого экранирования, разрешающих только входящий FTP-трафик.

Действие	**Команда**
Создание фильтра FTP, в правиле под номером 10 которого указывается, что необходимо помечать трафик с портом назначения 21/TCP	[edit] admin@edge# set filter FTP rule 10 destination port '21' [edit] admin@edge# set filter FTP rule 10 protocol 'tcp'
В этот же фильтр добавляются установленные (established) и ссылающиеся на установленные соединения (related). Последние используются для разрешения соединения данных. Данный механизм подходит как для активного, так и для пассивного режима работы FTP-сервера	[edit] admin@edge# set filter FTP rule 20 state established 'enable' [edit] admin@edge# set filter FTP rule 20 state related 'enable'
Фиксация изменений политики фильтрации	[edit] admin@edge# commit

Просмотр изменений	[edit]
	admin@edge-no-dm# show filter FTP
	rule 10 {
	destination {
	port 21
	}
	protocol tcp
	}
	rule 20 {
	state {
	established enable
	related enable
	}
	}

Создание политики межсетевого экранирования с именем FTP-only. Правило 10 разрешает трафик, попавший под ранее настроенную политику фильтрации FTP	[edit] admin@edge# set policy firewall FTP-only rule 10 action 'accept' [edit] admin@edge# set policy firewall FTP-only rule 10 match filter 'FTP'
Действие по умолчанию отбрасывает весь трафик, не попавший под настроенные правила	[edit] admin@edge# set policy firewall FTP-only default-action 'drop'
Фиксация изменений политики межсетевого экранирования	[edit] admin@edge# commit

Просмотр получившихся изменений	[edit]
	admin@edge# show policy firewall FTP-only
	default-action drop
	enable-default-log
	rule 10 {
	action accept
	match {

Действие	Команда
	filter FTP } }

3.4. Настройка правил NAT для работы FTP proxy в прозрачном режиме

Предположим, необходимо настроить FTP proxy таким образом, чтобы клиенты FTP не подозревали о его существовании. Данный метод реализуется с помощью так называемого «прозрачного режима». Для его реализации необходимо настроить правила NAT, перенаправляющие FTP-трафик, адресом назначения которого является FTP-сервер на FTP proxy.

Примечание. Для настройки данного метода используется IP-адресация как в примере 1 с тем лишь условием, что у устройств FTP-server и FTP-client есть маршруты до подсетей друг друга.

Для настройки FTP proxy в прозрачном режиме выполните следующие действия:

Пример 3 – Настройка правил NAT для работы в «прозрачном режиме»

Действие	Команда
Создание правила NAT, с номером 10 в режиме преобразования адреса получателя (DNAT)	[edit] admin@edge# set service nat ipv4 rule 10 type destination
Данное правило будет срабатывать для трафика, адресом назначения которого является 192.168.1.100 и портом назначения 21	[edit] admin@edge# set service nat ipv4 rule 10 destination address 192.168.1.100 [edit] admin@edge# set service nat ipv4 rule 10 destination port 21
При указании специфического порта обязательным условием является задание протокола, в данном случае TCP	[edit] admin@edge# set service nat ipv4 rule 10 protocol tcp
Для применения правил фильтрации данный трафик должен поступать на порт eth2	[edit] admin@edge# set service nat ipv4 rule 10 inbound-interface eth2
Данное правило фильтрации перенаправляет трафик, попавший под описание, на адрес 203.0.113.1 и порт 21. Этот адрес и порт прослушивает служба ftpproxy согласно настройкам в примере 1	[edit] admin@edge# set service nat ipv4 rule 10 inside-address address 203.0.113.1 [edit] admin@edge# set service nat ipv4 rule 10 inside-address port 21

4. КОМАНДЫ ФИЛЬТРАЦИИ FTP

Команда	**Описание**
service ftpproxy	Включение режима фильтрации FTP.
service ftpproxy auth-rules <номер_правила>	Определение правила доступа к FTP-серверу.
service ftpproxy auth-rules <номер_правила> action	Указание действия, которое должно быть выполнено для пакетов, соответствующих правилу доступа к FTP-серверу.
service ftpproxy auth-rules <номер_правила> description	Указание описания для правила доступа к FTP-серверу.
service ftpproxy auth-rules <номер_правила> destination	Указание адреса получателя и номера сетевого порта для проверки соответствия в правиле доступа к FTP-серверу.
service ftpproxy auth-rules <номер_правила> source	Указание адреса отправителя, по которому будет осуществляться проверка соответствия в правиле доступа к FTP-серверу.
service ftpproxy auth-rules <номер_правила> user <пользователь>	Указание имени пользователя в правиле доступа к FTP-серверу.
service ftpproxy command-rules <номер_правила>	Определение правила фильтрации команд FTP.
service ftpproxy command-rules <номер_правила> action	Указание действия, которое должно быть выполнено для пакетов, соответствующих правилу фильтрации команд FTP.
service ftpproxy command-rules <номер_правила> command	Указание команды FTP, которая должна содержаться в пакете для соответствия правилу фильтрации команд FTP.
service ftpproxy command-rules <номер_правила> description <описание>	Указание описания для правила фильтрации команд FTP.
service ftpproxy command-rules <номер_правила> destination	Указание адреса получателя и номера сетевого порта для проверки соответствия в правиле фильтрации команд FTP.
service ftpproxy command-rules <номер_правила> source	Указание адреса отправителя, по которому будет осуществляться проверка соответствия в правиле фильтрации команд FTP.
service ftpproxy command-rules <номер_правила> user <пользователь>	Указание имени пользователя в правиле фильтрации команд FTP.
service ftpproxy command-rules <номер_правила> wildcard <маска>	Указание маски для применения правил только к определенным файлам или каталогам.
service ftpproxy default-actions action	Указание действия, которое должно быть

Команда	Описание
	выполнено для пакетов, не попавших под настроенные правила.
service ftpproxy internal	Указание внутреннего адреса получателя и номера сетевого порта, на которых обрабатываются запросы клиентов.
service ftpproxy remote-server	Указание адреса или имени FTP-сервера.

4.1. service ftpproxy

Включение режима фильтрации FTP.

Синтаксис

```
set service ftpproxy
delete service ftpproxy
show service ftpproxy
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    ftpproxy {
    }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для включения режима фильтрации FTP в Numa Edge.
Форма **set** данной команды используется для включения режима фильтрации FTP.
Форма **delete** данной команды используется для отключения режима фильтрации FTP.
Форма **show** используется для отображения настройки.

4.2. service ftpproxy auth-rules <номер_правила>

Определение правила доступа к FTP-серверу.

Синтаксис

```
set service ftpproxy auth-rules <номер_правила>
delete service ftpproxy auth-rules <номер_правила>
show service ftpproxy auth-rules <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service ftpproxy {
   auth-rules 1-999 {}
}
```

Параметры

номер_правила

Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 999. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации auth-rules.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет определить правило доступа к FTP-серверу. Набор правил доступа может включать в себя до 999 настраиваемых правил. Правила доступа исполняются в порядке следования их номеров, от наименьшего к наибольшему. Для того чтобы не прибегать к изменению номеров правил, хорошей практикой является указание номеров с шагом 10. Это позволяет оставить пространство, куда можно будет впоследствии добавить новые правила.

Форма **set** данной команды используется для создания или изменения правила доступа к FTP-серверу.

Форма **delete** данной команды используется для удаления правила доступа к FTP-серверу.

Форма **show** данной команды используется для отображения настройки правила доступа к FTP-серверу.

4.3. service ftpproxy auth-rules <номер_правила> action

Указание действия, которое должно быть выполнено для пакетов, соответствующих правилу доступа к FTP-серверу.

Синтаксис

```
set service ftpproxy auth-rules <номер_правила> action {deny | permit}
delete service ftpproxy auth-rules <номер_правила> action
show service ftpproxy auth-rules <номер_правила> action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service ftpproxy {
   auth-rules 1-999 {
      action {
         deny
         permit
      }
  }
}
```

Параметры

номер_правила

Номер определенного правила доступа.

deny

Пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений.

permit

Пакеты, соответствующие данному правилу, пересылаются.

Значение по умолчанию

Пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений (**deny**).

Указания по использованию

Форма **set** этой команды используется для определения действия, выполняемого над пакетом, удовлетворяющим критериям соответствия в данном правиле. Если действием в правиле является deny, то пакеты, удовлетворяющие критериям соответствия правила, игнорируются без каких-либо действий и сообщений. Если действием в правиле является permit, то пакеты, удовлетворяющие критериям соответствия правила, пересылаются.

Форма **delete** этой команды используется для восстановления действия по умолчанию над пакетами, удовлетворяющими критериям соответствия.

Форма **show** этой команды используется для отображения параметров действия данного правила.

4.4. service ftpproxy auth-rules <номер_правила> description <описание>

Указание описания для правила доступа к FTP-серверу.

Синтаксис

```
set service ftpproxy auth-rules <номер_правила> description <описание>
delete set service ftpproxy auth-rules <номер_правила> description
show set service ftpproxy auth-rules <номер_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service ftpproxy {
    auth-rules 1-999 {
      description описание {
      }
   }
}
```

Параметры

description

Текстовое значение, в котором можно указать поясняющий комментарий для определенного правила.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания описания правила.

Форма **set** этой команды используется для указания описания правила.

Форма **delete** этой команды используется для удаления описания правила.

Форма **show** этой команды используется для просмотра описания правила.

4.5. service ftpproxy auth-rules <номер_правила> destination

Указание адреса получателя и номера сетевого порта для проверки соответствия в правиле доступа к FTP-серверу.

Синтаксис

```
set service ftpproxy auth-rules <номер_правила> destination [address
адрес | port порт ]
delete service ftpproxy auth-rules <номер_правила> destination
[address | port]
show service ftpproxy auth-rules <номер_правила> destination [address
| port]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service ftpproxy {
   auth-rules 1-999 {
      destination {
         address адрес
         port порт
      }
   }
}
```

Параметры

номер_правила

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 999.

адрес

Адрес назначения для проверки соответствия. Допустимые форматы:

- **IP-адрес**: IP-адрес сервера FTP;
- **IP-адрес/префикс**: адрес сети сервера FTP.

порт

Порт назначения для проверки соответствия. Поддерживаются следующие значения:

- **имя_порта**: проверка соответствия по названию службы IP; например, http. Названия различных служб можно указать в файле /etc/services;
- **номер_порта**: проверка соответствия по номеру порта. Значение должно лежать в диапазоне от 1 до 65535;
- **начало–конец**: проверка соответствия по номеру порта из указанного диапазона, например, 1001–1005.

Можно использовать сочетание этих форматов, указав список, разделенный запятыми. Также можно указать отрицание для всего списка, указав перед ним восклицательный знак («!»); например, !22,telnet,http,123,1001-1005.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать получателя в правиле фильтрации FTP. В том случае если явно указаны адрес и номер порта, для пакета устанавливается соответствие критериям правила в том и только том случае, если совпадает как адрес, так и номер порта.

Форма **set** данной команды позволяет указать или изменить получателя.

Форма **delete** данной команды позволяет удалить настройку получателя.

Форма **show** данной команды позволяет отобразить настройку получателя.

4.6. service ftpproxy auth-rules <номер_правила> source

Указание адреса отправителя, по которому будет осуществляться проверка соответствия в правиле доступа к FTP-серверу.

Синтаксис

```
set service ftpproxy auth-rules номер_правила source [address адрес]
delete service ftpproxy auth-rules номер_правила source [address]
show service ftpproxy auth-rules номер_правила source [address]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service ftpproxy {
    auth-rules 1-999 {
       source {
         address адрес
       }
    }
}
```

Параметры

номер_правила

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 999.

адрес

Адрес отправителя для проверки соответствия. Поддерживаются следующие форматы:

- **IP-адрес**: адрес клиента FTP;
- **IP-адрес/префикс**: адрес сети, где 0.0.0.0/0 соответствует любой сети.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать адрес источника, по которому будет осуществляться проверка соответствия пакета критериям правила доступа к FTP-серверу.

Форма **set** используется для создания адреса отправителя для правила фильтрации FTP.

Форма **delete** данной команды используется для удаления настройки отправителя для правила фильтрации FTP.

Форма **show** данной команды используется для отображения настройки отправителя.

4.7. service ftpproxy auth-rules <номер_правила> user <пользователь>

Указание имени пользователя в правиле доступа к FTP-серверу.

Синтаксис

```
set service ftpproxy auth-rules <номер_правила> user <пользователь>
delete set service ftpproxy auth-rules <номер_правила> user
<пользователь>
show set service ftpproxy auth-rules <номер_правила> user
<пользователь>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service ftpproxy {
    auth-rules 1-999 {
      user пользователь {
      }
    }
}
```

Параметры

пользователь

Множественный узел. Уникальный идентификатор пользователя, допускаются алфавитно-цифровые символы и дефисы. Можно определить несколько учетных записей пользователей, создав несколько узлов конфигурации user.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания имени пользователя.
Форма **set** этой команды используется для задания имени пользователя.
Форма **delete** этой команды используется для удаления имени пользователя.
Форма **show** этой команды используется для просмотра настройки имени пользователя.

4.8. service ftpproxy command-rules <номер_правила>

Определение правила фильтрации команд FTP.

Синтаксис

```
set service ftpproxy command-rules <номер_правила>
delete service ftpproxy command-rules <номер_правила>
show service ftpproxy command-rules <номер_правила>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service ftpproxy {
   command-rules 1-999 {}
}
```

Параметры

номер_правила
Множественный узел. Численный идентификатор правила. Номера правил определяют порядок, в котором они применяются. Каждое правило должно иметь уникальный номер. Значение должно лежать в диапазоне от 1 до 999. В том случае если необходимо определить несколько правил, следует создать соответствующее количество узлов конфигурации command-rules.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет определить правило фильтрации команд FTP. Набор правил доступа может включать в себя до 999 настраиваемых правил. Правила фильтрации команд исполняются в порядке следования их номеров, от наименьшего к наибольшему. Для того чтобы не прибегать к изменению номеров правил, хорошей практикой является указание номеров с шагом 10. Это позволяет оставить пространство, куда можно будет впоследствии добавить новые правила.

Форма **set** данной команды используется для создания или изменения правила фильтрации команд FTP.

Форма **delete** данной команды используется для удаления правила фильтрации команд FTP.

Форма **show** данной команды используется для отображения настройки правила фильтрации команд FTP.

4.9. service ftpproxy command-rules <номер_правила> action

Указание действия, которое должно быть выполнено для пакетов, соответствующих правилу команд фильтрации FTP.

Синтаксис

```
set service ftpproxy command-rules <номер_правила> action {deny |
permit}
delete service ftpproxy command-rules <номер_правила> action
show service ftpproxy command-rules <номер_правила> action
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service ftpproxy {
   command-rules 1-999 {
      action {
         deny
         permit
      }
  }
}
```

Параметры

номер_правила

Номер определенного правила доступа.

deny

Пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений.

permit

Пакеты, соответствующие данному правилу, пересылаются.

Значение по умолчанию

Пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений (**deny**).

Указания по использованию

Форма **set** этой команды используется для определения действия, выполняемого над пакетом, удовлетворяющим критериям соответствия в данном правиле. Если действием в правиле является deny, то пакеты, удовлетворяющие критериям соответствия правила, игнорируются без каких-либо действий и сообщений. Если действием в правиле является permit, то пакеты, удовлетворяющие критериям соответствия правила, пересылаются.

Форма **delete** этой команды используется для восстановления действия по умолчанию над пакетами, удовлетворяющими критериям соответствия.

Форма **show** этой команды используется для отображения параметров действия данного правила.

4.10. service ftpproxy command-rules <номер_правила> command

Указание команды FTP, которая должна содержаться в пакете для соответствия правилу фильтрации команд FTP.

Синтаксис

```
set service ftpproxy command-rules <номер_правила> command <текст>
delete service ftpproxy command-rules <номер_правила> command
show service ftpproxy command-rules <номер_правила> command
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service ftpproxy {
   command-rules 1-999 {
     command текст
   }
}
```

Параметры

номер_правила

Номер определенного правила доступа.

текст

Команда FTP. Множественный узел. Допустимы следующие значения: APPE, CDUP, CWD, DELE, LIST, MDTM, MKD, NLST, RETR, RNFR, RNTO, RMD, SIZE, STAT, STOR, STOU, XCUP, XCWD, XMKD, XRMD.

Значение по умолчанию

Отсутствует.

Указания по использованию

Форма **set** этой команды используется для определения команды FTP.
Форма **delete** этой команды используется для удаления команды FTP
Форма **show** этой команды используется для отображения заданных команд FTP.

4.11. service ftpproxy command-rules <номер_правила> description <описание>

Указание описания для правила фильтрации команд FTP.

Синтаксис

```
set service ftpproxy command-rules <номер_правила> description
<описание>
delete set service ftpproxy command-rules <номер_правила> description
show set service ftpproxy command-rules <номер_правила> description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service ftpproxy {
    command-rules 1-999 {
      description описание {
      }
   }
}
```

Параметры

description

Текстовое значение, в котором можно указать поясняющий комментарий для определенного правила.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания описания правила.
Форма **set** этой команды используется для указания описания правила.
Форма **delete** этой команды используется для удаления описания правила.
Форма **show** этой команды используется для просмотра описания правила.

4.12. service ftpproxy command-rules <номер_правила> destination

Указание адреса получателя и номера сетевого порта для проверки соответствия в правиле фильтрации команд FTP.

Синтаксис

```
set service ftpproxy command-rules <номер_правила> destination
[address адрес | port порт ]
delete service ftpproxy command-rules <номер_правила> destination
[address | port]
show service ftpproxy command-rules <номер_правила> destination
[address | port]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service ftpproxy {
   command-rules 1-999 {
      destination {
         address адрес
         port порт
      }
   }
}
```

Параметры

номер_правила

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 999.

адрес

Адрес назначения для проверки соответствия. Допустимые форматы:

- **ip-адрес**: IP-адрес сервера FTP;
- **ip-адрес/префикс**: адрес сети сервера FTP.

порт

Порт назначения для проверки соответствия. Поддерживаются следующие значения:

- **имя_порта**: проверка соответствия по названию службы IP; например, http. Названия различных служб можно указать в файле /etc/services;
- **номер_порта**: проверка соответствия по номеру порта. Значение должно лежать в диапазоне от 1 до 65535;
- **начало–конец**: проверка соответствия по номеру порта из указанного диапазона, например, 1001–1005.

Можно использовать сочетание этих форматов, указав список, разделенный запятыми. Также можно указать отрицание для всего списка, указав перед ним восклицательный знак («!»); например, !22,telnet,http,123,1001-1005.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать получателя в правиле фильтрации команд FTP. В том случае если явно указаны адрес и номер порта, для пакета устанавливается соответствие критериям правила в том и только том случае, если совпадает как адрес, так и номер порта.

Форма **set** данной команды позволяет указать или изменить получателя.

Форма **delete** данной команды позволяет удалить настройку получателя.

Форма **show** данной команды позволяет отобразить настройку получателя.

4.13. service ftpproxy command-rules <номер_правила> source

Указание адреса отправителя, по которому будет осуществляться проверка соответствия в правиле фильтрации команд FTP.

Синтаксис

```
set service ftpproxy command-rules номер_правила source [address
адрес]
delete service ftpproxy command-rules номер_правила source [address]
show service ftpproxy command-rules номер_правила source [address]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service ftpproxy {
    command-rules 1-999 {
       source {
         address адрес
       }
   }
}
```

Параметры

номер_правила

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 999.

адрес

Адрес назначения для проверки соответствия. Допустимые форматы:

- **ip-адрес**: IP-адрес сервера FTP;
- **ip-адрес/префикс**: адрес сети сервера FTP, где 0.0.0.0/0 соответствует любой сети.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать адрес источника, по которому будет осуществляться проверка соответствия пакета критериям правила фильтрации команд FTP.

Форма **set** используется для создания адреса отправителя для правила фильтрации команд FTP.

Форма **delete** данной команды используется для удаления настройки отправителя для правила фильтрации команд FTP.

Форма **show** данной команды используется для отображения настройки отправителя.

4.14. service ftpproxy command-rules <номер_правила> user <пользователь>

Указание имени пользователя в правиле фильтрации команд FTP.

Синтаксис

```
set service ftpproxy command-rules <номер_правила> user
<пользователь>
delete set service ftpproxy command-rules <номер_правила> user
<пользователь>
show set service ftpproxy command-rules <номер_правила> user
<пользователь>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service ftpproxy {
    command-rules 1-999 {
      user пользователь {
      }
   }
}
```

Параметры

пользователь

Множественный узел. Уникальный идентификатор пользователя, допускаются алфавитно-цифровые символы и дефисы. Можно определить несколько учетных записей пользователей, создав несколько узлов конфигурации user.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания имени пользователя.

Форма **set** этой команды используется для задания имени пользователя.

Форма **delete** этой команды используется для удаления имени пользователя.

Форма **show** этой команды используется для просмотра настройки имени пользователя.

4.15. service ftpproxy command-rules <номер_правила> wildcard <маска>

Указание маски для применения правил только к определенным файлам или каталогам.

Синтаксис

```
set service ftpproxy command-rules <номер_правила> wildcard  <маска>
delete set service ftpproxy command-rules <номер_правила> wildcard
<маска>
show set service ftpproxy command-rules <номер_правила> wildcard
<маска>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service ftpproxy {
    command-rules 1-999 {
      wildcard маска {
      }
   }
}
```

Параметры

маска

Множественный узел. Задает маску имени файла или каталога, к которому будет применена команда из данного правила. Маска может работать только со следующими командами: 'APPE', 'CWD', 'DELE', 'LIST', 'MKD', 'NLST', 'RETR', 'RMD', 'RNFR', 'RNTO', 'STOR'.

Значение по умолчанию

Отсутствует.

Указания по использованию

Эта команда используется для указания файла или каталога, к которому будет применена команда. Доступны следующие значения:

- текстовое описание относительного имени файла или каталога;

- [] – описывается диапазон символов для сопоставления одного символа в этом диапазоне;
- ? – не в скобках соответствует одиночному символу;
- * – не в скобках соответствует любому количеству символов, в том числе и их отсутствию;
- ! – если указывается в скобках первым символом, то соответствует отрицанию данного диапазона;
- \ – экранирование, используется в скобках для сопоставления со спецсимволами.

Форма **set** этой команды используется для задания файла или имени каталога, к которому применяется команда.

Форма **delete** этой команды используется для удаления файла или имени каталога, к которому применяется команда.

Форма **show** этой команды используется для просмотра файла или имени каталога, к которому применяется команда.

4.16. service ftpproxy default-actions action

Указание действия, которое должно быть выполнено для пакетов, не попавших под настроенные правила.

Синтаксис

```
set service ftpproxy default-actions {deny | permit}
delete service ftpproxy default-actions
show service ftpproxy default-actions
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service ftpproxy {
   default-actions {
         deny
         permit
  }
}
```

Параметры

deny

Пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений.

permit

Пакеты, соответствующие данному правилу, пересылаются.

Значение по умолчанию

По умолчанию пакеты игнорируются без каких-либо действий и сообщений (deny).

Указания по использованию

Форма **set** этой команды используется для определения действия, выполняемого над пакетом, не попавшим ни под одно из правил. Если действием является deny, то пакеты игнорируются без каких-либо действий и сообщений. Если действием является permit, то пакеты пересылаются.

Форма **delete** этой команды используется для восстановления действия по умолчанию над пакетами, не попавших под настроенные правила.

Форма **show** этой команды используется для отображения параметров действия для пакетов, не попавших под настроенные правила.

4.17. service ftpproxy internal

Указание внутреннего адреса получателя и номера сетевого порта, на которых обрабатываются запросы клиентов.

Синтаксис

```
set service ftpproxy internal [address адрес | port порт ]
delete service ftpproxy internal [address | port]
show service ftpproxy internal [address | port]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service ftpproxy {
   internal {
      address адрес
        port порт
      }
   }
}
```

Параметры

адрес

Внутренний адрес. Допустимые форматы:

- **IP-адрес**: внутренний IP-адрес.

порт

Внутренний порт. Поддерживаются следующие значения:

- **номер_порта**: проверка соответствия по номеру порта. Значение должно лежать в диапазоне от 1 до 65535.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать внутренний адрес и порт, на которых обрабатываются запросы клиентов.

Форма **set** данной команды позволяет указать или изменить внутренний адрес и порт.

Форма **delete** данной команды позволяет удалить настройку внутреннего адреса и порта.

Форма **show** данной команды позволяет отобразить настройку внутреннего адреса и порта.

4.18. service ftpproxy remote-server

Указание адреса или имени FTP-сервера.

Синтаксис

```
set service ftpproxy remote-server <сервер>
delete service ftpproxy remote-server
show service ftpproxy remote-server
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service ftpproxy {
    remote-server сервер
}
```

Параметры

сервер
Адрес или имя FTP-сервера.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать адрес или имя FTP-сервера.

Форма **set** данной команды позволяет изменить адрес или имя FTP-сервера.

Форма **delete** данной команды позволяет удалить настройку адреса или имени FTP-сервера.

Форма **show** данной команды позволяет отобразить настройку адреса или имени FTP-сервера.

Межсетевой экран Numa Edge

Руководство администратора

Настройка VPN с использованием протоколов PPTP и L2TP/IPSec

Листов 48

Санкт-Петербург
2022

СОДЕРЖАНИЕ

ИДЕНТИФИКАЦИЯ ДОКУМЕНТА

Название документа	Руководство администратора. Настройка VPN с использованием протоколов PPTP и L2TP/IPSec
Версия документа	1.0
Идентификация ОО	Межсетевой экран Numa Edge
Идентификация разработчика	ООО «НумаТех»
Ключевые слова	Межсетевой экран, МЭ, PPTP, L2TP/IPSec

ВВЕДЕНИЕ

Данный документ описывает примеры настройки протоколов L2TP и PPTP для обеспечения удаленного доступа посредством туннелирования соединения и шифрования данных. Numa Edge VPN так же поддерживает реализации OpenVPN и IPSec, примеры конфигурации которых описаны в других документах.

1. ОПИСАНИЕ ПРОТОКОЛОВ PPTP И L2TP

1.1. PPTP

PPTP (Point-to-Point Tunneling Protocol) — туннельный протокол типа «точка-точка», позволяющий компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в стандартной незащищённой сети. Спецификация протокола PPTP приведена в RFC 2637. Протокол считается менее безопасным, чем другие протоколы, используемые для построения VPN, например, IPSec.

Безопасность решения PPTP напрямую зависит от сложности паролей, которые используются пользователями. По этой причине при использовании в практических условиях следует внимательно следить за стойкостью используемых паролей. Как следствие этого, решения на базе PPTP слабее по сравнению с другими решениями.

К преимуществам данной технологии построения VPN можно отнести простоту настройки, а также тот факт, что все версии ОС Microsoft Windows, начиная с Windows 95 OSR2, включают в свой состав встроенный клиент PPTP.

На рисунке 1 приведена схема использования режима удаленного доступа VPN с использованием PPTP.

Рисунок 1 - VPN удаленного доступа на основе протокола PPTP

При использовании такого решения:

- Клиент PPTP устанавливает соединение TCP с сервером (порт 1723).
- Через установленное соединение клиент PPTP и сервер устанавливают туннель GRE (Generic Routing Encapsulation).
- Затем поверх туннеля GRE устанавливается сеанс протокола PPP (Point-to-Point Protocol): пакеты PPP инкапсулируются и принимаются/отправляются через туннель GRE.

Аутентификация пользователей и шифрование данных осуществляется на уровне PPP при помощи комбинации имени и пароля с использованием протокола MS CHAP или MS CHAP v2 для аутентификации и протокола MPPE для шифрования.

1.2. L2TP/IPSec

L2TP (Layer 2 Tunneling Protocol) — туннельный протокол, использующийся для поддержки виртуальных частных сетей. Для обеспечения безопасности пакетов L2TP используется набор протоколов IPSec, который обеспечивает конфиденциальность, аутентификацию и целостность передаваемых данных.

После запуска сервера L2TP начинается прослушивание порта UDP/1701 на предмет входящих соединений L2TP на внешнем интерфейсе сервера VPN. В штатном режиме работы клиент VPN первым устанавливает сеанс IPSec с сервером VPN, после чего через туннель IPSec устанавливается соединение L2TP.

При прослушивании порта UDP/1701 L2TP сервер также принимает входящие подключения L2TP, которые не туннелируются при помощи IPSec. Это может быть использовано, например, в том случае, если пользователь устанавливает соединение L2TP VPN без туннеля IPSec (следует отметить, что клиенты VPN под управлением ОС Windows не имеют такой возможности), при этом весь трафик пользователя будет «открытым», то есть не будет шифроваться.

На рисунке 2 приведен режим VPN удаленного доступа с использованием протокола L2TP (Layer 2 Tunneling Protocol) и IPSec.

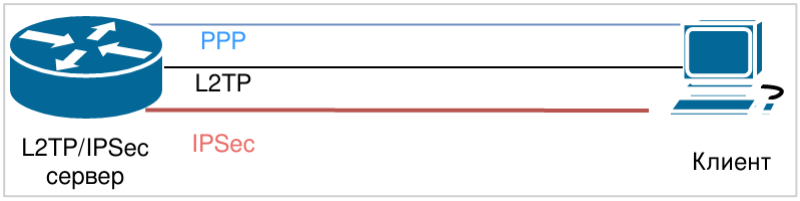


Рисунок 2 - VPN удаленного доступа на основе протокола L2TP/IPSec

При использовании такого решения:

- Удаленный компьютер сначала устанавливает туннель IPSec к серверу VPN.
- Затем клиент и сервер L2TP устанавливают туннель L2TP поверх туннеля IPSec.
- Далее сеанс PPP устанавливается поверх туннеля L2TP: пакеты PPP инкапсулируются и принимаются/отправляются через туннель L2TP.

В практических условиях рекомендуется ограничивать использование L2TP соединений без использования IPSec. В зависимости от ситуации этого можно добиться следующими способами:

- В том случае если сервер VPN размещается в демилитаризованной зоне (DMZ) и перед ним установлен межсетевой экран, то межсетевой экран может быть настроен на прохождение к серверу VPN только трафика IPSec (то есть прохождение пакетов на UDP порт 1701 запрещено). Таким образом, соединения L2TP/IPSec смогут быть установлены, а соединения L2TP будут заблокированы.
- В том случае если сервер VPN напрямую подключен ко внешней сети, межсетевой экран на сервере VPN должен быть настроен таким образом, чтобы запрещать отдельные соединения L2TP. Например, для того чтобы разрешить подключения L2TP/IPSec, можно определить в системе следующее правило и применить его к внешнему интерфейсу с использованием ключевого слова **local** (правило в этом случае будет применяться к пакетам, предназначенным для системы Numa Edge). Соединения L2TP без использования IPSec могут быть заблокированы правилом **default-drop**.

```
rule 10 {
   action accept
      destination {
         port 1701
      }
      ipsec {
         match-ipsec
      }
      protocol udp
   }
```

1.3. L2TP/IPSec с использованием предварительных ключей

Настройка режима с использованием предварительных ключей проще, чем настройка режима с использованием сертификатов стандарта X.509. Следует учесть, что всеми удаленными пользователями VPN в части IPSec их подключений должны быть использованы одинаковые предварительные ключи, что может создавать определенные трудности — например, когда доступ VPN необходимо отозвать у одного из пользователей. Несмотря на то, что доступ можно ограничить на основе более высокоуровневой аутентификации, пользователь все же будет обладать ключом IPSec и сможет устанавливать сеансы IPSec, что нежелательно. Для того чтобы предотвратить такую ситуацию, необходимо будет настроить новый ключ на сервере VPN и всех клиентах VPN.

В этом случае на уровне PPP (с использованием имени и пароля) осуществляется только аутентификация пользователей. Шифрование данных обеспечивается средствами IPSec. Более того, чтобы осуществить шифрование, IPSec также требует аутентификации (использование IPSec в режиме, при котором осуществляется только шифрование, считается менее безопасным).

При использовании L2TP/IPSec с аутентификацией на основе предварительных ключей на всех удаленных клиентах должны быть настроены одинаковые ключи. Следовательно, при смене ключа необходимо будет настраивать заново все удаленные клиенты. Использование аутентификации на основе сертификатов стандарта X.509 позволяет избежать указанной ситуации.

1.4. L2TP/IPSec с использованием сертификатов стандарта X.509

Использование сертификатов X.509 совместно с L2TP/IPSec позволит предотвратить вышеупомянутую ситуацию, однако применение сертификатов имеет свои сложности:

- Сертификаты стандарта X.509 необходимо создавать с использованием инфраструктуры открытых ключей (PKI) при помощи удостоверяющего центра (CA). Для этого могут использоваться PKI, созданные при помощи коммерческих или свободно распространяемых продуктов (например, OpenSSL), а также модуля PKI системы Numa Edge. Установка PKI требует комплексного подхода к вопросам безопасности.
- После получения сертификатов необходимо решить вопрос безопасной доставки сертификатов удаленным пользователям. Для этого, например, можно записать сертификаты на USB-флеш-накопитель и перенести их на каждое из клиентских устройств. Также сертификаты можно передать по протоколу SCP.
- При использовании сертификатов X.509 с L2TP/IPSec, настройка клиентов VPN в ОС Windows сложнее, чем при использовании предварительных ключей. По этой причине, а также из-за проблемы распределения сертификатов, может возникнуть необходимость предварительной настройки компьютеров клиентов для организации удаленного доступа.

Общая схема работы L2TP/IPSec VPN с использованием сертификатов X.509 функционирует следующим образом:

1. Сетевой администратор получает сертификат, подписанный удостоверяющим центром для каждого удаленного пользователя, и распространяет их пользователям через безопасные каналы совместно с пользовательскими открытыми/секретными ключами.
2. Сетевой администратор настраивает сервер VPN с открытым ключом удостоверяющего центра.
3. Когда удаленный клиент подключается к серверу VPN, он предоставляет свой сертификат.
4. Сервер VPN подтверждает подлинность сертификата при помощи открытого ключа удостоверяющего центра. В результате успешной проверки подлинности сервер получает открытый ключ клиента. Впоследствии сервер может использовать данный открытый ключ для аутентификации.
5. В результате успешной аутентификации устанавливается туннель IPSec между клиентом и сервером, после чего этапы использования L2TP и PPP аналогичны тем, которые применяются при аутентификации с помощью предварительных ключей.

2. ПРИМЕРЫ КОНФИГУРАЦИИ L2TP И PPTP

2.1. Пример построения VPN на базе протокола PPTP

На первом этапе настройки удаленного доступа клиента под управлением ОС Windows 10 на базе протокола PPTP необходимо настроить систему Numa Edge в качестве сервера PPTP. В примере 1 настраиваемая система имеет имя edge1. Предполагается, что на устройстве edge1 настроен внешний IP-адрес 203.0.113.1 и внутренний IP-адрес 192.168.10.254. За данным устройством располагается внутренняя сеть с адресом 192.168.10.0/24, к которой необходимо обеспечить доступ для удаленного пользователя. На рисунке 3 представлена схема данной сети.

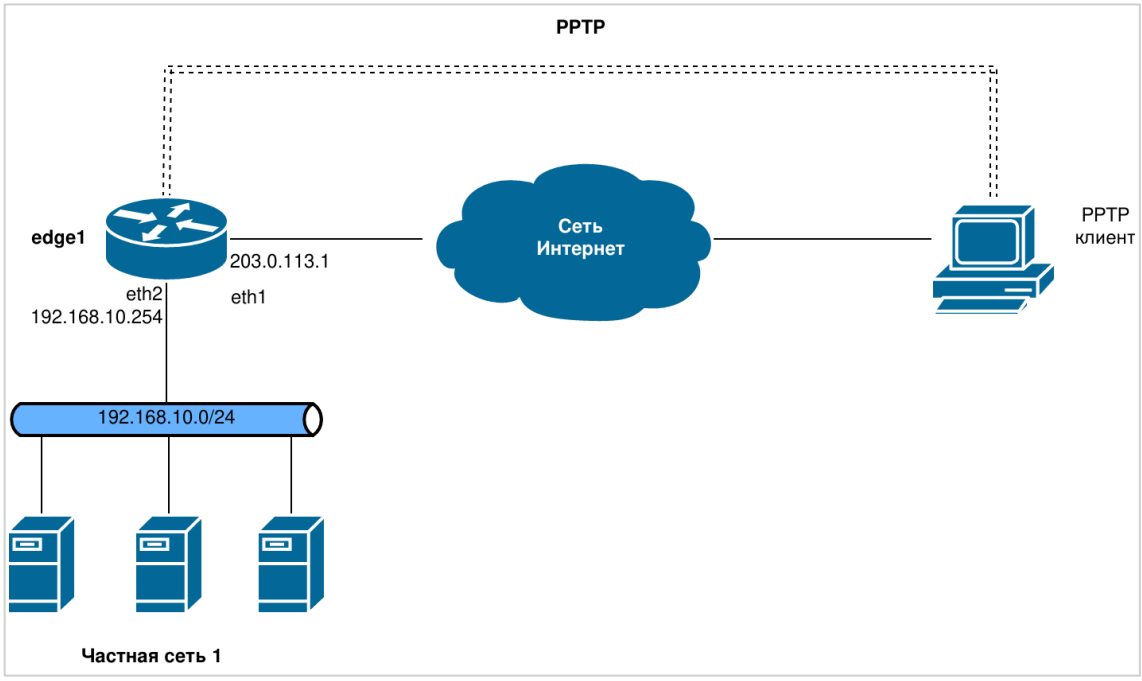


Рисунок 3 – Схема подключения клиента PPTP

Для того чтобы настроить сервер PPTP, необходимо выполнить следующие действия на устройстве edge1 в режиме настройки:

Пример 1 - VPN удаленного доступа на базе протокола PPTP

Действие	Команда
Привязка сервера PPTP ко внешнему адресу.	`[edit]` `admin@edge1# set vpn pptp listen-on address 203.0.113.1`

Установка пула IP-адресов, которые будут присваиваться удаленным клиентам.
В этом случае доступными будут 10 адресов в диапазоне от .101 до .110.
	`[edit]`
	`admin@edge1# set vpn pptp client-ip-pool start 192.168.10.101`
	`[edit]`
	`admin@edge1# set vpn pptp client-ip-pool stop 192.168.10.110`

Установка режима аутентификации - в данном случае режима локальной аутентификации (local).	`[edit]` `admin@edge1# set vpn pptp authentication mode local`
Установка имени пользователя (testuser) и пароля (testpassword).	`[edit]` `admin@edge1# set vpn pptp authentication local-users username testuser password testpassword`
Фиксация изменений.	`[edit]` `admin@edge1# commit`

Действие	Команда

Вывод настройки.	[edit]
	admin@edge1# show vpn pptp
	authentication {
	local-users {
	username testuser {
	password testpassword
	}
	}
	mode local
	}
	client-ip-pool {
	start 192.168.10.101
	stop 192.168.10.110
	}
	listen-on {
	address 203.0.113.1
	}

Следующим шагом является настройка клиента PPTP VPN в ОС Windows 10.

1. Нажмите на **значок уведомлений** в правом нижнем углу экрана
2. Выберите **Виртуальная сеть (VPN)**.
3. В новом окне **Параметры** выберите **Добавить VPN-подключение**.
4. Укажите следующие данные:
   a. **Поставщик услуг VPN** - Windows (встроенные).
   b. **Имя подключения** - удобное для вас имя подключения, например, PPTP.
   c. **Имя или адрес сервера** - 203.0.113.1.
   d. **Тип VPN** - Автоматически или PPTP.
   e. **Тип данных для входа** - Имя пользователя и пароль.
   f. **Имя пользователя** - testuser
   g. **Пароль** - testpassword
   h. Поставьте галочку напротив **Запомнить мои данные для входа**.
   i. Нажмите **Сохранить**.
5. Выберите Подключиться.
6. Дождитесь окончания подключения и закройте окно Параметры.

ПРИМЕЧАНИЕ: Следует убедиться в том, что между удаленным клиентом и сервером не блокируются пакеты протокола GRE или пакеты TCP, имеющие порт назначения с номером 1723. (Необходимо проверить настройки межсетевого экрана, шлюз, модем DSL, ISP, и т.д.)

2.2. Пример построения VPN на базе L2TP/IPSec с использованием аутентификации на основе предварительных ключей

На первом этапе настройки удаленного доступа необходимо настроить систему Numa Edge в качестве сервера VPN на основе L2TP/IPSec. В данном примере настраиваемая система имеет имя edge1. Предполагается, что на устройстве edge1 настроен внешний IP-адрес 203.0.113.1 и внутренний IP-адрес 192.168.10.254. За данным устройством располагается внутренняя сеть с адресом 192.168.10.0/24, к которой необходимо обеспечить доступ для удаленного пользователя. Схема сети в данном случае полностью соответствует схеме на рисунке 1 за исключением того, что используется другой протокол для настройки VPN соединения.

Пример 2 - VPN удаленного доступа с использованием L2TP/IPSec

Действие	Команда
Привязка сервера L2TP ко внешнему адресу.	`[edit]` `admin@edge1# set vpn l2tp  listen-on address 203.0.113.1`

Установка пула IP-адресов, которые будут присваиваться удаленным клиентам VPN.
В данном случае доступными будут 10 адресов - от .101 до .110.
	`[edit]`
	`admin@edge1# set vpn l2tp client-ip-pool start 192.168.10.101`
	`[edit]`
	`admin@edge1# set vpn l2tp client-ip-pool stop 192.168.10.110`

Установка использования предварительных ключей в качестве режима аутентификации IPSec.	`[edit]` `admin@edge1# set vpn l2tp ipsec-settings authentication method pre-shared-key`
Установка предварительно распределяемого ключа.	`[edit]` `admin@edge1# set vpn l2tp ipsec-settings authentication pre-shared-key !secrettext!`
Установка режима аутентификации L2TP в «local».	`[edit]` `admin@edge1# set vpn l2tp authentication mode local`
Указание имени пользователя и пароля для удаленного доступа L2TP.	`[edit]` `admin@edge1# set vpn l2tp authentication local-users username testuser password testpassword`
Фиксация изменений.	`[edit]` `admin@edge1# commit`

Вывод настройки удаленного доступа l2tp.	`[edit]`
	`admin@edge-no-dm# show vpn l2tp`
	`  authentication {`
	`  local-users {`
	`  username testuser {`
	`  password testpassword`
	`  }`
	`  }`
	`  mode local`
	`  }`
	`  client-ip-pool {`
	`  start 192.168.10.101`
	`  stop 192.168.10.110`
	`  }`
	`  ipsec-settings {`
	`  authentication {`
	`  method pre-shared-key`
	`  pre-shared-key !secrettext!`
	`  }`
	`  }`
	`  listen-on {`
	`  address 203.0.113.1`
	`  }`

Следующим шагом является настройка клиента L2TP/IPSec в ОС Windows 10.

1. Нажмите на **значок уведомлений** в правом нижнем углу экрана.
2. Выберите **Виртуальная сеть (VPN)**.
3. В новом окне **Параметры** выберите **Добавить VPN-подключение**.
4. Укажите следующие данные:

a. **Поставщик услуг VPN** - Windows (встроенные).
b. **Имя подключения** - удобное для вас имя подключения, например, L2TP.
c. **Имя или адрес сервера** - 203.0.113.1.
d. **Тип VPN** - L2TP/IPsec с предварительным ключом.
e. **Общий ключ** - !secrettext!.
f. **Тип данных для входа** - Имя пользователя и пароль.
g. **Имя пользователя** - testuser.
h. **Пароль** - testpassword.
i. **Поставьте галочку** напротив **Запомнить мои данные для входа**.
j. Нажмите **Сохранить**.

5. Выберите Подключиться.

ПРИМЕЧАНИЕ: Следует убедиться в том, что между удаленным клиентом и сервером нет ничего, что могло бы блокировать пакеты протокола L2TP или порт UDP с номером 500. (Необходимо проверить настройки межсетевого экрана, шлюз, модем DSL, ISP, и т.д.)

2.3. Настройка трафика Интернет при использовании VPN

На компьютерах с установленной ОС Windows по умолчанию после создания настройки VPN устанавливается маршрут по умолчанию через туннель VPN. Это означает, что, например, Интернет-трафик будет маршрутизироваться через VPN. В том случае, если требуется сохранить текущий маршрут для Интернет-трафика, необходимо настроить VPN следующим образом:

1. Следует выбрать **Start (Пуск)** → **Control Panel (Панель управления)** → **Network and Sharing Center (Центр управления сетями и общим доступом)**.
2. Нажать правой кнопкой мыши на значке подключения **VPN** (**«PPTP»** в первом примере). Выбрать **Properties (Свойства)**.
3. Выбрать вкладку **Networking (Сеть)**. Выбрать **«IP версии 4 (TCP/IPv4)»**, затем нажать на кнопку **Properties (Свойства)**.
4. Нажать на кнопку **Advanced (Дополнительно)**. Снять флажок **«Use default gateway on remote network» (Использовать основной шлюз в удаленной сети)**.
5. Нажать на кнопку **OK** три раза.

3. КОМАНДЫ VPN ПРОТОКОЛОВ L2TP И PPTP

В этом разделе приведены следующие команды.

Таблица 1 - Команды VPN протоколов L2TP и PPTP

Команды настройки	
Сервер L2TP	
vpn l2tp	Создание узла конфигурации для L2TP VPN.
vpn l2tp authentication mode <режим>	Указание режима аутентификации пользователей для подключений L2TP VPN.
vpn l2tp authentication metod <метод>	Указание метода аутентификации пользователей для подключений L2TP VPN.
vpn l2tp authentication local-users username <имя_пользователя>	Указание имени пользователя для аутентификации удаленных пользователей L2TP VPN.
vpn l2tp client-ip-pool start <ipv4-адрес>	Указание начального адреса пула IP-адресов, которые будут назначаться удаленным клиентам L2TP VPN.
vpn l2tp client-ip-pool stop <ipv4-адрес>	Указание конечного адреса пула IP-адресов, которые будут назначаться удаленным клиентам L2TP VPN.
vpn l2tp description <описание>	Указание описания для узла конфигурации сервера L2TP VPN.
vpn l2tp dns-servers server-1 <ipv4-адрес>	Указание IP-адреса основного сервера DNS для удаленных клиентов L2TP VPN.
vpn l2tp dns-servers server-2 <ipv4-адрес>	Указание IP-адреса вторичного сервера DNS для удаленных клиентов L2TP VPN.
vpn l2tp ipsec-settings authentication method <режим>>	Установка режима, который будет использоваться при IPSec аутентификации подключений удаленного доступа L2TP VPN.
vpn l2tp ipsec-settings authentication pre-shared-key <ключ>	Установка предварительного ключа, используемого при аутентификации IPSec подключений удаленного доступа L2TP VPN.
vpn l2tp ipsec-settings authentication x509-cert <имя_сертификата>	Указание сертификата X.509, используемого при аутентификации IPSec подключений удаленного доступа L2TP VPN.
vpn l2tp listen-on <ipv4-адрес>	Указание внешнего IP-адреса сервера L2TP, на котором будут ожидаться входящие подключения.
vpn l2tp local-ip <ipv4-адрес>	Назначение внутреннего туннельного IP-адреса на сервере L2TP.
vpn l2tp mru <значение>	Указание значения максимального размера получаемой полезной нагрузки.
vpn l2tp mtu <значение>	Указание значения максимального размера передаваемой полезной нагрузки.
vpn l2tp policy [arp|ethernet|firewall|firewall-ipv6] <имя_политики>	Применение различных политик для трафика, передаваемого через L2TP VPN.
vpn l2tp remote <ipv4-сеть>	Указание подсети с которой возможно подключение к L2TP VPN серверу.
vpn l2tp server-name <имя_сервера>	Указание имени сервера L2TP, которое передается клиенту по ходу процедуры аутентификации.

vpn l2tp wins-servers server-1 <ipv4-адрес>	Указание IP-адреса основного сервера WINS для удаленных клиентов L2TP VPN.
vpn l2tp wins-servers server-2 <ipv4-адрес>	Указание IP-адреса вторичного сервера WINS для удаленных клиентов L2TP VPN.
Сервер PPTP	
vpn pptp	Создание узла настойки PPTP VPN.
vpn pptp authentication mode <режим>	Указание режима аутентификации пользователей для подключений PPTP VPN.
vpn pptp authentication local-users username <имя_пользователя> password <пароль>	Указание имени пользователя и пароля для аутентификации удаленных пользователей PPTP VPN.
vpn pptp client-ip-pool start <ipv4-адрес>	Указание начального адреса пула IP-адресов, которые будут назначаться удаленным клиентам PPTP VPN.
vpn pptp client-ip-pool stop <ipv4-адрес>	Указание конечного адреса пула IP-адресов, которые будут назначаться удаленным клиентам PPTP VPN.
vpn pptp description <описание>	Указание описания для узла конфигурации сервера PPTP VPN.
vpn pptp dns-servers server-1 <ipv4-адрес>	Указание IP-адреса основного сервера DNS для удаленных клиентов PPTP VPN.
vpn pptp dns-servers server-2 <ipv4-адрес>	Указание IP-адреса вторичного сервера DNS для удаленных клиентов PPTP VPN.
vpn pptp listen-on <ipv4-адрес>	Указание внешнего IP-адреса сервера PPTP, на котором будут ожидаться входящие подключения.
vpn pptp local-ip <ipv4-адрес>	Назначение внутреннего туннельного IP-адреса на сервере PPTP.
vpn pptp policy [arp|ethernet|firewall|firewall-ipv6] <имя_политики>	Применение различных политик для трафика, передаваемого через L2TP VPN.
vpn pptp wins-servers server-1 <ipv4-адрес>	Указание IP-адреса основного сервера WINS для удаленных клиентов PPTP VPN.
vpn pptp wins-servers server-2 <ipv4-адрес>	Указание IP-адреса вторичного сервера WINS для удаленных клиентов PPTP VPN.
Клиент PPTP	
interfaces pptp <pptpx>	Создание узла конфигурации клиента PPTP в системе Numa Edge.
interfaces pptp <pptpx> domain <домен>	Установить имя домена, используемого при аутентификации.
interfaces pptp <pptpx> mppe-stateless <состояние>	Установить режим протокола MPPE.
interfaces pptp <pptpx> nomppe-128 <состояние>	Установить режим использования протокола MPPE с ключом длиной 128 бит.
interfaces pptp <pptpx> nomppe-40 <состояние>	Установить режим использования протокола MPPE с ключом длиной 40 бит.
interfaces pptp <pptpx> password <пароль>	Указание пароля, который будет использован для аутентификации.
interfaces pptp <pptpx> reconnect <состояние>	Установка режима автоматического восстановления подключения в случае разрыва соединения.

interfaces pptp <pptpx> refuse-eap <состояние>	Установить режим использования протокола EAP для аутентификации.
interfaces pptp <pptpx> remote-name <имя>	Указание имени удаленного узла, которое может использоваться для аутентификации.
interfaces pptp <pptpx> require-mppe <состояние>	Установить режим обязательного шифрования данных с использованием протокола MPPE.
interfaces pptp <pptpx> server <ipv4-адрес>	Указание IP-адреса сервера PPTP.
interfaces pptp <pptpx> usepeerdns <состояние>	Установить режим запроса адресов серверов DNS у сервера PPTP.
interfaces pptp <pptpx> username <имя_пользователя>	Указание имени пользователя, которое будет использовано при аутентификации.
Эксплуатационные команды	
clear vpn remote-access user <имя_пользователя>	Завершение активного сеанса указанного пользователя.
show vpn remote-access	Вывод сведений о текущих активных сеансах удаленного доступа VPN.

3.1. vpn l2tp

Создание узла конфигурации L2TP VPN.

Синтаксис

```
set vpn l2tp
delete vpn l2tp
show vpn l2tp
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
    l2tp
   }
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для создания узла конфигурации протокола L2TP, что позволяет включить L2TP в системе Numa Edge.

Форма **set** данной команды используется для создания узла конфигурации L2TP VPN.

Форма **delete** данной команды используется для удаления настройки L2TP VPN.

Форма **show** данной команды используется для отображения настройки L2TP VPN.

3.2. vpn l2tp authentication metod <метод>

Указание метода аутентификации пользователя по протоколу PPP.

Синтаксис

```
set vpn l2tp authentication metod <метод>
delete vpn l2tp authentication metod
show vpn l2tp authentication metod
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
    l2tp {
        authentication {
            metod [pap|chap|mschapv1|mschapv2]
        }
    }
}
```

Параметры

режим

Обязательный. Режим аутентификации удаленных пользователей. Поддерживаются следующие значения:

- **pap**: Использовать метод PAP (Password Authentication Protocol), описанный в RFC 1334.
- **chap**: Использовать метод CHAP (Challenge Handshake Authentication Protocol), описанный в RFC 1994.
- **mschapv1:** Использовать реализацию метода CHAP от компании Microsoft.
- **mschapv2:** Использовать улучшенную реализацию метода CHAP от компании Microsoft.

Значение по умолчанию

По умолчанию используется метод аутентификации **mschapv2**. Обратите внимание, что при использовании аутентификации на стороннем LDAP сервере для метода **pap** проверка осуществляется на этом сервере, в то время как для различных реализаций **chap** – информация о пароле передается на Numa Edge. В этом случае на Numa Edge осуществляется проверка правильности логина и пароля пользователя.

Указания по использованию

Данная команда используется для указания метода аутентификации удаленных пользователей L2TP VPN.

Форма **set** данной команды используется для настройки режима аутентификации пользователей.

Форма **delete** данной команды используется для удаления указанного режима аутентификации.

Форма **show** данной команды используется для отображения режима аутентификации пользователей.

3.3. vpn l2tp authentication mode <режим>

Указание режима аутентификации пользователей для подключений L2TP VPN.

Синтаксис

```
set vpn l2tp authentication mode <режим>
delete vpn l2tp authentication mode
show vpn l2tp authentication mode
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    l2tp {
        authentication {
            mode [local|ldap]
```

```
            }
        }
    }
```

Параметры

режим

Обязательный. Режим аутентификации удаленных пользователей. Поддерживаются следующие значения:

- **local**: Локальная аутентификация пользователей.
- **ldap**: Аутентификация посредством сервера LDAP.

Значение по умолчанию

Пользователи проходят аутентификацию с использованием локальной базы данных пользователей, определенной в настройке **l2tp vpn**.

Указания по использованию

Данная команда используется для указания типа аутентификации удаленных пользователей L2TP VPN.

Пользователи могут быть аутентифицированы локально с использованием учетных данных, указанных с помощью команды **vpn l2tp authentication local-users username** <*имя_пользователя*> или с использованием сервера LDAP. Если указывается режим аутентификации с использованием сервера LDAP, необходимо настроить параметры сервера LDAP с помощью команды **system ldap-server**.

Форма **set** данной команды используется для настройки режима аутентификации пользователей.

Форма **delete** данной команды используется для удаления указанного режима аутентификации.

Форма **show** данной команды используется для отображения режима аутентификации пользователей.

3.4. vpn l2tp authentication local-users username <имя_пользователя>

Указание имени пользователя для аутентификации удаленных пользователей L2TP VPN.

Синтаксис

```
set vpn l2tp authentication local-users username <имя_пользователя>
[disable | password пароль]
delete vpn l2tp authentication local-users username <имя_пользователя>
[disable | password]
show vpn l2tp authentication local-users username <имя_пользователя>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
    l2tp {
        authentication {
            local-users {
                username текст {
                    disable
                    password текст
                }
            }
        }
    }
}
```

Параметры

имя_пользователя

Имя пользователя. Обязательный, если установлен режим локальной аутентификации (для узла **authentication mode** установлено значение **local**).

disable

Отключение удаленного доступа для пользователя.

пароль

Пароль для указанного пользователя. Обязательный, если установлен режим локальной аутентификации (для узла **authentication mode** установлено значение **local**).

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания учетных записей удаленных пользователей L2TP VPN.

Форма **set** данной команды используется для создания узла конфигурации имени пользователя.

Форма **delete** данной команды используется для удаления учетной записи пользователя.

Форма **show** данной команды используется для отображения настройки.

3.5. vpn l2tp client-ip-pool start <ipv4-адрес>

Указание начального адреса пула IP-адресов, которые назначаются удаленным клиентам L2TP VPN.

Синтаксис

```
set vpn l2tp client-ip-pool start <ipv4-адрес>
delete vpn l2tp client-ip-pool start
show vpn l2tp client-ip-pool start
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
    l2tp {
        client-ip-pool {
            start ipv4-адрес
        }
    }
}
```

Параметры

ipv4-адрес

Обязательный. Начальный IP-адрес пула адресов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать начальный адрес пула адресов для удаленных пользователей L2TP VPN. При подключении удаленным клиентам будут назначаться IP-адреса из пула адресов, начальный адрес которого задается командой **vpn l2tp client-ip-pool start** <*ipv4-адрес*>, а конечный адрес задается командой **vpn l2tp client-ip-pool stop** <*ipv4-адрес*>. Каждый подключенный клиент должен иметь уникальный адрес, поэтому в пуле адресов должно быть

определено, по меньшей мере, столько адресов, сколько предполагается одновременно подключенных клиентов. Рекомендуется выбирать диапазон адресов с некоторым запасом, поскольку значение этого параметра нельзя изменить без перезапуска сервера L2TP.

Обязательно должны быть указаны начальный адрес и конечный адрес.

Форма **set** данной команды используется для определения начального адреса.

Форма **delete** данной команды используется для удаления указанного начального адреса.

Форма **show** данной команды используется для отображения начального адреса.

3.6. vpn l2tp client-ip-pool stop <ipv4-адрес>

Указание конечного адреса пула IP-адресов, которые будут назначаться удаленным клиентам L2TP VPN.

Синтаксис

```
set vpn l2tp client-ip-pool stop <ipv4-адрес>
delete vpn l2tp client-ip-pool stop
show vpn l2tp client-ip-pool stop
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
    l2tp {
        client-ip-pool {
             stop ipv4-адрес
        }
    }
}
```

Параметры

ipv4-адрес

Обязательный. Конечный адрес пула IP-адресов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать конечный адрес пула IP-адресов для удаленных клиентов L2TP VPN.

При подключении удаленным клиентам будут назначаться IP-адреса из пула адресов, начальный адрес которого задается командой **vpn l2tp client-ip-pool start** <*ipv4-адрес*>, а конечный адрес задается командой **vpn l2tp client-ip-pool stop** <*ipv4-адрес*>. Каждый подключенный клиент должен иметь уникальный адрес, поэтому в пуле адресов должно быть определено, по меньшей мере, столько адресов, сколько предполагается одновременно подключенных клиентов. Рекомендуется выбирать диапазон адресов с некоторым запасом, поскольку значение этого параметра нельзя изменить без перезапуска сервера L2TP.

Обязательно должны быть указаны начальный адрес и конечный адрес.

Форма **set** данной команды используется для указания конечного адреса.

Форма **delete** данной команды используется для удаления указанного конечного адреса.

Форма **show** данной команды используется для отображения конечного адреса.

3.7. vpn l2tp description <описание>

Задание описания для VPN соединения.

Синтаксис

```
set vpn l2tp description <описание>
delete vpn l2tp description
show vpn l2tp description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    l2tp {
        description описание
    }
}
```

Параметры

описание

Текстовое описание, используемое для идентификации узла конфигурации L2TP VPN сервера.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для задания текстового описания. Полезно при использовании нескольких различных конфигураций L2TP VPN серверов.

Форма **set** данной команды используется для задания текстового описания.

Форма **delete** данной команды используется для удаления текстового описания.

Форма **show** данной команды используется для отображения текстового описания.

3.8. vpn l2tp dns-servers server-1 <ipv4-адрес>

Указание IP-адреса основного сервера DNS для удаленных клиентов L2TP VPN.

Синтаксис

```
set vpn l2tp dns-servers server-1 <ipv4-адрес>
delete vpn l2tp dns-servers server-1
show vpn l2tp dns-servers server-1
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
    l2tp {
        dns-servers {
           server-1 ipv4-адрес
        }
    }
}
```

Параметры

ipv4-адрес

IP-адрес основного сервера DNS для удаленных клиентов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания основного сервера DNS для удаленных клиентов L2TP VPN.

Форма **set** данной команды используется для указания IP-адреса основного сервера DNS.

Форма **delete** данной команды используется для удаления IP-адреса основного сервера DNS.

Форма **show** данной команды используется для отображения IP-адреса основного сервера DNS.

3.9. vpn l2tp dns-servers server-2 <ipv4-адрес>

Указание IP-адреса вторичного сервера DNS для удаленных клиентов L2TP VPN.

Синтаксис

```
set vpn l2tp dns-servers server-2 <ipv4-адрес>
delete vpn l2tp dns-servers server-2
show vpn l2tp dns-servers server-2
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    l2tp {
        dns-servers {
            server-2 ipv4-адрес
        }
    }
}
```

Параметры

ipv4-адрес
IP-адрес вторичного сервера DNS для удаленных клиентов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания вторичного сервера DNS для удаленных клиентов L2TP VPN.

Форма **set** данной команды используется для указания IP-адреса основного сервера DNS.

Форма **delete** данной команды используется для удаления IP-адреса вторичного сервера DNS.

Форма **show** данной команды используется для отображения IP-адреса вторичного сервера DNS.

3.10. vpn l2tp ipsec-settings authentication method <режим>

Установка режима, который будет использоваться при IPSec аутентификации подключений удаленного доступа L2TP VPN.

Синтаксис

```
set vpn l2tp ipsec-settings authentication method <режим>
delete vpn l2tp ipsec-settings authentication method
show vpn l2tp ipsec-settings authentication method
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    l2tp {
        ipsec-settings {
            authentication {
                method [pre-shared-key|x509]
            }
        }
    }
}
```

Параметры

режим

Обязательный. Установка режима IPSec аутентификации для удаленных подключений L2TP VPN. Поддерживаются следующие значения:

- **pre-shared-key**: Использование предварительных ключей для аутентификации.
- **x509**: Использование сертификатов стандарта X.509 V.3 для аутентификации.

Значение по умолчанию

По умолчанию установлен режим аутентификации с использованием предварительных ключей.

Указания по использованию

Данная команда позволяет установить режим аутентификации IPSec для удаленных подключений L2TP VPN.

По умолчанию установлен режим аутентификации с использованием предварительных ключей (PSK). В качестве предварительного ключа используется строка, заранее согласованная обеими сторонами для аутентификации сеанса. Она используется для создания хеш-значения, чтобы оконечные точки могли аутентифицировать друг друга.

При установке режима аутентификации с использованием предварительных ключей необходимо настроить ключ с помощью команды **vpn l2tp ipsec-settings authentication pre-shared-key** <*ключ*>.

Предварительный ключ не передается между оконечными точками. На обеих сторонах должен быть настроен один и тот же ключ. Режим использования предварительных ключей является менее безопасным по сравнению с режимом, использующим сертификаты стандарта X.509.

ПРИМЕЧАНИЕ Следует использовать предварительные ключи только в малых сетях с низким уровнем опасности.

Сертификаты X.509 v.3 представляют собой сертификаты, соответствующие стандарту ITU-T X.509 версии 3 для инфраструктуры открытых ключей (PKI). Сертификат выпускается удостоверяющим центром (CA) и безопасно хранится в локальной системе Numa Edge.

При установке режима аутентификации с использованием сертификатов стандарта X.509 необходимо настроить все сведения для сертификата X.509.

Форма **set** данной команды используется для указания режима аутентификации для удаленных подключений L2TP VPN.

Форма **delete** данной команды используется для удаления настройки режима аутентификации.

Форма **show** данной команды используется для отображения режима аутентификации.

3.11. vpn l2tp ipsec-settings authentication pre-shared-key <ключ>

Установка предварительного ключа, используемого при IPSec аутентификации подключений удаленного доступа L2TP VPN.

Синтаксис

```
set vpn l2tp ipsec-settings authentication pre-shared-key <ключ>
delete vpn l2tp ipsec-settings authentication pre-shared-key
show vpn l2tp ipsec-settings authentication pre-shared-key
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    l2tp {
        ipsec-settings {
            authentication {
                pre-shared-key текст
            }
        }
    }
}
```

Параметры

ключ

Ключ или пароль, который используется для аутентификации удаленного подключения. Указание этого параметра является обязательным, если установлен режим аутентификации с использованием предварительных ключей (для параметра **authentication method** установлено значение **pre-shared-key**). На обеих сторонах подключения должен быть указан один и тот же ключ.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для установки предварительного ключа, используемого для аутентификации IPSec подключений удаленного доступа L2TP VPN.

Форма **set** данной команды используется для указания предварительного ключа.

Форма **delete** данной команды используется для удаления настройки предварительного ключа.

Форма **show** данной команды используется для отображения настройки предварительного ключа.

3.12. vpn l2tp ipsec-settings authentication x509-cert <имя_сертификата>

Указание имени сертификата X.509 в модуле PKI, используемого при аутентификации IPSec подключений удаленного доступа L2TP VPN.

Синтаксис

```
set vpn l2tp ipsec-settings authentication x509-cert <имя_сертификата>
delete vpn l2tp ipsec-settings authentication x509-cert
show vpn l2tp ipsec-settings authentication x509-cert
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    l2tp {
```

```
            ipsec-settings {
                authentication {
                    x509-cert текст
                }
            }
        }
    }
```

Параметры

имя_сертификата

Имя сертификата. Обязательный, если установлен режим аутентификации с использованием PKI (для параметра **authentication method** установлено значение **x509**).

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать сертификат X.509. Данный сертификат используется при аутентификации IPSec подключений удаленного доступа L2TP VPN.

Форма **set** данной команды используется для указания сертификата.

Форма **delete** данной команды используется для удаления настройки сертификата.

Форма **show** данной команды используется для отображения настройки сертификата.

3.13. vpn l2tp listen-on <ipv4-адрес>

Указание внешнего IP-адреса сервера L2TP, на котором будут ожидаться входящие подключения.

Синтаксис

```
set vpn l2tp listen-on <ipv4-адрес>
delete vpn l2tp listen-on
show vpn l2tp listen-on
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    l2tp {
        listen-on ipv4-адрес
    }
}
```

Параметры

ipv4-адрес

Обязательный. IPv4-адрес сервера L2TP, на котором будут ожидаться входящие подключения.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для установки внешнего адреса для подключений удаленного доступа L2TP VPN.

Под внешним адресом подразумевается адрес интерфейса, обращенного к внешней сети. Сервер L2TP будет принимать подключения, приходящие только на указанный адрес.

Форма **set** данной команды используется для установки внешнего адреса L2TP VPN.

Форма **delete** данной команды используется для удаления настройки внешнего адреса L2TP VPN.

Форма **show** данной команды используется для отображения настройки внешнего адреса L2TP VPN.

3.14. vpn l2tp local-ip <ipv4-адрес>

Назначение внутреннего туннельного IP-адреса на сервере L2TP.

Синтаксис

```
set vpn l2tp local-ip <ipv4-адрес>
delete vpn l2tp local-ip
show vpn l2tp local-ip
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    l2tp {
        local-ip ipv4-адрес
    }
}
```

Параметры

ipv4-адрес

Обязательный. IPv4-адрес который будет назначаться L2TP VPN серверу на туннельном интерфейсе.

Значение по умолчанию

По умолчанию используется адрес 10.255.255.0.

Указания по использованию

Данная команда используется для изменения IP-адреса туннельного интерфейса на L2TP VPN сервере.

Форма **set** данной команды используется для установки IP-адреса туннельного интерфейса на L2TP VPN сервере.

Форма **delete** данной команды используется для удаления IP-адреса туннельного интерфейса на L2TP VPN сервере. После удаления используется значение по умолчанию.

Форма **show** данной команды используется для отображения IP-адреса туннельного интерфейса на L2TP VPN сервере.

3.15. vpn l2tp mru <значение>

Указание максимального размера получаемой полезной нагрузки для L2TP VPN соединения.

Синтаксис

```
set vpn l2tp mru <значение>
delete vpn l2tp mru
show vpn l2tp mru
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    l2tp {
        mru значение
```

```
        }
    }
```

Параметры

значение

Обязательный. Значение MRU (Maximum resive unit) в байтах.

Значение по умолчанию

По умолчанию используется значение 1400 байт.

Указания по использованию

Данная команда используется для задания значения MRU. При расчете значения необходимо иметь в виду размеры заголовков пакетов, в которые инкапсулируется L2TP VPN трафик. В общем случае рекомендуется указывать одинаковые значения для MTU и MRU. Для Ethernet по умолчанию значение MTU=1500; заголовки IP – 20 байт, заголовки UDP – 8 байт, заголовки L2TP – 16 байт, заголовок PPP – 2 байта, размера заголовков ESP – 20 байт. Таким образом минимальный размер MRU, получаемого с Ethernet интерфейса с установленным MTU 1500 равен 1500-20-8-16-2-20=1434.

Форма **set** данной команды используется для задания значения MRU трафика L2TP VPN.

Форма **delete** данной команды используется для удаления значения MRU трафика L2TP VPN.

Форма **show** данной команды используется для отображения значения MRU трафика L2TP VPN.

3.16. vpn l2tp mtu <значение>

Указание максимального размера передаваемой полезной нагрузки для L2TP VPN соединения.

Синтаксис

```
set vpn l2tp mtu <значение>
delete vpn l2tp mtu
show vpn l2tp mtu
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    l2tp {
        mtu значение
    }
}
```

Параметры

значение

Обязательный. Значение MTU (Maximum transmit unit) в байтах.

Значение по умолчанию

По умолчанию используется значение 1400 байт.

Указания по использованию

Данная команда используется для задания значения MTU. При расчете значения необходимо иметь в виду размеры заголовков пакетов, в которые инкапсулируется L2TP VPN трафик. В общем случае рекомендуется указывать одинаковые значения для MTU и MRU. Для Ethernet по умолчанию значение MTU=1500; заголовки IP – 20 байт, заголовки UDP – 8 байт, заголовки L2TP – 16 байт, заголовок PPP – 2 байта, размера заголовков ESP – 20 байт. Таким образом

минимальный размер MRU, получаемого с Ethernet интерфейса с установленным MTU 1500 равен 1500-20-8-16-2-20=1434.

Форма **set** данной команды используется для задания значения MTU трафика L2TP VPN.

Форма **delete** данной команды используется для удаления значения MTU трафика L2TP VPN.

Форма **show** данной команды используется для отображения значения MTU трафика L2TP VPN.

3.17. vpn l2tp policy [arp|ethernet|firewall|firewall-ipv6] <имя_политики>

Указание максимального размера передаваемой полезной нагрузки для L2TP VPN соединения.

Синтаксис

```
set vpn l2tp policy [in|local|out] [arp|clone|clone-
ipv6|ethernet|firewall|firewall-ipv6|route| route-ipv6] <имя_политики>
delete vpn l2tp policy [in|local|out] [arp|clone|clone-
ipv6|ethernet|firewall|firewall-ipv6|route| route-ipv6]
show vpn l2tp policy [in|local|out] [arp|clone|clone-
ipv6|ethernet|firewall|firewall-ipv6|route| route-ipv6]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    l2tp {
        policy [in|local|out] {
            [arp|clone|clone-ipv6|ethernet|firewall|firewall-
ipv6|route|route-ipv6] имя_политики
        }
    }
}
```

Параметры

направление трафика

in: Входящий транзитный трафик, адресом назначения которого являются другие внешние узлы, а источником – L2TP VPN клиенты.

out: Исходящий транзитный трафик, адресом назначения которого являются источником L2TP VPN клиенты, а источником – другие внешние узлы.

local: Входящий локальный трафик, адресом назначения которого является L2TP VPN сервер, а источником могут быть как и L2TP VPN клиенты, так и другие внешние узлы.

тип политики

arp: Политика фильтрации ARP входящего трафика.

clone: Политика клонирования IPv4 трафика для интерфейса. (Не работает для направления **local**)

clone-ipv6: Политика клонирования IPv6 трафика для интерфейса. (Не работает для направления **local**)

ethernet: Политика фильтрации Ethernet входящего трафика. (Работает только для интерфейса, объединенного в мост)

firewall: Политика МЭ IPv4.

firewall-ipv6: Политика МЭ IPv6.

route: Политика маршрутизации IPv4 трафика для интерфейса**.** (Не работает для направления **local**)

route-ipv6: Политика маршрутизации IPv6 трафика для интерфейса. (Не работает для направления local)

имя политики

Имя существующей политики, применяемое для заданного направления.

Значение по умолчанию

Отсутствует

Указания по использованию

Используется для управления трафика, передаваемого через L2TP VPN соединение.

Форма **set** данной команды используется для задания политик трафика, передаваемого через L2TP VPN.

Форма **delete** данной команды используется для удаления политик трафика, передаваемого через L2TP VPN.

Форма **show** данной команды используется для просмотра заданных политик трафика, передаваемого через L2TP VPN.

3.18. vpn l2tp remote <ipv4-сеть>

Указание подсети, с которой возможно установить соединение с L2TP VPN сервером.

Синтаксис

```
set vpn l2tp remote <ipv4-сеть>
delete vpn l2tp remote
show vpn l2tp remote
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
    l2tp {
        remote ipv4-сеть
    }
}
```

Параметры

ipv4-адрес

Обязательный. IPv4-подсеть с которой разрешается установить соединение с L2TP VPN сервером.

Значение по умолчанию

По умолчанию отсутствует ограничение на IP-адрес источника пакетов для установления соединения, т.е значение равно 0.0.0.0/0.

Указания по использованию

Данная команда позволяет указать подсеть IPv4 из которой разрешено устанавливать соединение с L2TP VPN сервером. По идее использования похоже на правила фильтрации с по адресу назначения, однако работает на уровне самого процесса L2TP VPN сервера.

Форма **set** данной команды используется для указания подсети, с которой возможно установить соединение с L2TP VPN сервером.

Форма **delete** данной команды используется для удаления подсети, с которой возможно установить соединение с L2TP VPN сервером. После удаления используется значение по умолчанию

Форма **show** данной команды используется для отображения подсети, с которой возможно установить соединение с L2TP VPN серве

3.19. vpn l2tp server-name <имя_сервера>

Указание имени сервера L2TP, которое передается клиенту по ходу процедуры аутентификации.

Синтаксис

```
set vpn l2tp  server-name <имя_сервера>
delete vpn l2tp  server-name
show vpn l2tp server-name
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    l2tp {
        server-name текст
    }
}
```

Параметры

имя_сервера
Обязательный параметр.

Значение по умолчанию

По умолчанию установлено значение openl2tpd.

Указания по использованию

Данная команда позволяет указать имя сервера L2TP, передающееся клиенту по ходу процедуры аутентификации. Клиент может использовать данное имя для аутентификации сервера.

Форма **set** данной команды используется для указания имени сервера L2TP.

Форма **delete** данной команды используется для удаления конфигурации.

Форма **show** данной команды используется для отображения конфигурации.

3.20. vpn l2tp wins-servers server-1 <ipv4-адрес>

Указание IP-адреса основного сервера WINS для удаленных клиентов L2TP VPN.

Синтаксис

```
set vpn l2tp wins-servers server-1 <ipv4-адрес>
delete vpn l2tp wins-servers server-1
show vpn l2tp wins-servers server-1
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    l2tp {
         wins-servers {
              server-1 ipv4-адрес
         }
     }
}
```

Параметры

ipv4-адрес
IP-адрес основного сервера WINS для удаленных клиентов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать IP-адрес основного сервера WINS для удаленных клиентов L2TP VPN. WINS (Windows Internet Name Service) - служба сопоставления NetBIOS-имён компьютеров с IP-адресами узлов.

Форма **set** данной команды используется для указания IP-адреса основного сервера WINS.

Форма **delete** данной команды используется для удаления IP-адреса основного сервера WINS.

Форма **show** данной команды используется для отображения IP-адреса основного сервера WINS.

3.21. vpn l2tp wins-servers server-2 <ipv4-адрес>

Указание IP-адреса вторичного сервера WINS для удаленных клиентов L2TP VPN.

Синтаксис

```
set vpn l2tp wins-servers server-2 <ipv4-адрес>
delete vpn l2tp wins-servers server-2
show vpn l2tp wins-servers server-2
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    l2tp {
        wins-servers {
            server-2 ipv4-адрес
        }
    }
}
```

Параметры

ipv4-адрес

IP-адрес вторичного сервера WINS для удаленных клиентов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать вторичный сервера WINS для удаленных клиентов L2TP VPN. WINS (Windows Internet Name Service) - служба сопоставления NetBIOS-имён компьютеров с IP-адресами узлов.

Форма **set** данной команды используется для указания IP-адреса вторичного сервера WINS.

Форма **delete** данной команды используется для удаления IP-адреса вторичного сервера WINS.

Форма **show** данной команды используется для отображения IP-адреса вторичного сервера WINS.

3.22. vpn pptp

Создание узла настойки PPTP VPN.

Синтаксис

```
set vpn pptp
delete vpn pptp
```

```
show vpn pptp
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    pptp
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для создания узла конфигурации для протокола PPTP (Point-to-Point Tunneling Protocol), что позволяет включить функциональность PPTP VPN в системе Numa Edge.

Форма **set** данной команды используется для создания узла конфигурации PPTP VPN.
Форма **delete** данной команды используется для удаления настройки PPTP VPN.
Форма **show** данной команды используется для отображения настройки PPTP VPN.

3.23. vpn pptp authentication mode <режим>

Указание режима аутентификации пользователей для подключений PPTP VPN.

Синтаксис

```
set vpn pptp authentication mode <режим>
delete vpn pptp authentication mode
show vpn pptp authentication mode
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    pptp {
        authentication {
            mode [local|ldap]
        }
    }
}
```

Параметры

режим

Обязательный. Режим аутентификации удаленных пользователей. Поддерживаются следующие значения:

- **local:** Локальная аутентификация пользователей.
- **ldap:** Аутентификация посредством сервера LDAP.

Значение по умолчанию

Пользователи проходят аутентификацию с использованием локальной базы данных пользователей, определенной в настройке **pptp vpn**.

Указания по использованию

Данная команда используется для указания типа аутентификации удаленных пользователей PPTP VPN.

Пользователи могут быть аутентифицированы локально, с использованием учетных данных, указанных с помощью команды **vpn pptp authentication local-users username <***имя_пользователя***> password <***пароль***>** (см. стр. 2217), или с использованием сервера LDAP.

Если применяется аутентификация с использованием сервера LDAP необходимо определить настройки сервера LDAP с помощью команды **system ldap-server**.

Форма **set** данной команды используется для настройки режима аутентификации.

Форма **delete** данной команды используется для удаления режима аутентификации.

Форма **show** данной команды используется для отображения режима аутентификации.

3.24. vpn pptp authentication local-users username <имя_пользователя> password <пароль>

Указание имени пользователя и пароля для аутентификации удаленных пользователей PPTP VPN.

Синтаксис

```
set vpn pptp authentication local-users username <имя_пользователя>
password <пароль>
delete vpn pptp authentication local-users username <имя_пользователя>
[password]
show vpn pptp authentication local-users username <имя_пользователя>
[password]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    pptp {
        authentication {
            local-users {
                username текст {
                    password текст
                }
            }
        }
    }
}
```

Параметры

имя_пользователя

Имя пользователя. Обязательный, если установлен режим локальной аутентификации (для параметра **authentication mode** установлено значение **local**).

пароль

Пароль, связанный с указанным именем пользователя. Обязательный, если установлен режим локальной аутентификации (для параметра **authentication mode** установлено значение **local**).

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания сведений о пользователе для удаленного доступа по PPTP VPN, которые будут использоваться при локальной аутентификации.

Форма **set** данной команды используется для создания узла конфигурации пользователя и установки пароля для пользователя.

Форма **delete** данной команды используется для удаления узла конфигурации пользователя или пароля.

Форма **show** данной команды используется для отображения узла конфигурации пользователя или пароля.

3.25. vpn pptp client-ip-pool start <ipv4-адрес>

Указание начального адреса пула IP-адресов, которые будут назначаться удаленным клиентам PPTP VPN.

Синтаксис

```
set vpn pptp client-ip-pool start <ipv4-адрес>
delete vpn pptp client-ip-pool start
show vpn pptp client-ip-pool start
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    pptp {
        client-ip-pool {
            start ipv4-адрес
        }
    }
}
```

Параметры

ipv4-адрес

Обязательный. Начальный IP-адрес пула адресов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания начального IP-адреса пула адресов, из которого будут назначаться адреса удаленным клиентам PPTP VPN.

В обязательном порядке должны быть указаны начальный адрес и конечный адрес пула IP-адресов. Для указания конечного адреса используется команда **vpn pptp client-ip-pool stop** <*ipv4-адрес*>.

Форма **set** данной команды используется для определения начального адреса.

Форма **delete** данной команды используется для удаления настройки начального адреса.

орма **show** данной команды используется для отображения начального адреса.

3.26. vpn pptp client-ip-pool stop <ipv4-адрес>

Указание конечного адреса пула IP-адресов, которые будут назначаться удаленным клиентам PPTP VPN.

Синтаксис

```
set vpn pptp client-ip-pool stop <ipv4-адрес>
delete vpn pptp client-ip-pool stop
show vpn pptp client-ip-pool stop
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
```

```
        pptp {
            client-ip-pool {
                stop ipv4-адрес
            }
        }
    }
```

Параметры

ipv4-адрес
Обязательный. Конечный адрес пула IP-адресов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания конечного адреса пула IP-адресов, из которого будут назначаться адреса удаленным клиентам PPTP VPN. В обязательном порядке должны быть указаны начальный адрес и конечный адрес пула адресов.

Для указания начального адреса используется команда **vpn pptp client-ip-pool start** <*ipv4-адрес*>.

Форма **set** данной команды используется для указания конечного адреса.

Форма **delete** данной команды используется для удаления конечного адреса.

Форма **show** данной команды используется для отображения конечного адреса.

3.27. vpn pptp description <описание>

Задание описания для VPN соединения.

Синтаксис

```
set vpn pptp description <описание>
delete vpn pptp description
show vpn pptp description
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    pptp {
        description описание
    }
}
```

Параметры

описание
Текстовое описание, используемое для идентификации узла конфигурации PPTP VPN сервера.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для задания текстового описания. Полезно при использовании нескольких различных конфигураций PPTP VPN серверов.

Форма **set** данной команды используется для задания текстового описания.

Форма **delete** данной команды используется для удаления текстового описания.

Форма **show** данной команды используется для отображения текстового описания.

3.28. vpn pptp dns-servers server-1 <ipv4-адрес>

Указание IP-адреса основного сервера DNS для удаленных клиентов PPTP VPN.

Синтаксис

```
set vpn pptp dns-servers server-1 <ipv4-адрес>
delete vpn pptp dns-servers server-1
show vpn pptp dns-servers server-1
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    pptp {
        dns-servers {
            server-1 ipv4-адрес
        }
    }
}
```

Параметры

ipv4-адрес
IP-адрес основного сервера DNS для удаленных клиентов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания основного сервера DNS для удаленных клиентов PPTP VPN.

Форма **set** данной команды используется для указания IP-адреса основного сервера DNS.

Форма **delete** данной команды используется для удаления IP-адреса основного сервера DNS.

Форма **show** данной команды используется для отображения IP-адреса основного сервера DNS.

3.29. vpn pptp dns-servers server-2 <ipv4-адрес>

Указание IP-адреса вторичного сервера DNS для удаленных клиентов PPTP VPN.

Синтаксис

```
set vpn pptp dns-servers server-2 <ipv4-адрес>
delete vpn pptp dns-servers server-2
show vpn pptp dns-servers server-2
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    pptp {
        dns-servers {
            server-2 ipv4-адрес
         }
    }
}
```

Параметры

ipv4-адрес

IP-адрес вторичного сервера DNS для удаленных клиентов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания вторичного сервера DNS для удаленных клиентов.

Форма **set** данной команды используется для указания IP-адреса вторичного сервера DNS.

Форма **delete** данной команды используется для удаления IP-адреса вторичного сервера DNS.

Форма **show** данной команды используется для отображения IP-адреса вторичного сервера DNS.

3.30. vpn pptp listen-on <ipv4-адрес>

Указание внешнего IP-адреса сервера PPTP, на котором будут ожидаться входящие подключения.

Синтаксис

```
set vpn pptp listen-on <ipv4-адрес>
delete vpn pptp listen-on
show vpn pptp listen-on
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    pptp {
        listen-on ipv4-адрес
    }
}
```

Параметры

ipv4-адрес

Обязательный. IPv4-адрес сервера PPTP, на котором будут ожидаться входящие подключения.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для установки внешнего адреса для подключений удаленного доступа PPTP VPN.

Под внешним адресом подразумевается адрес интерфейса, обращенного к внешней сети. Сервер PPTP будет принимать подключения, приходящие только на указанный адрес.

Форма **set** данной команды используется для установки внешнего адреса PPTP VPN.

Форма **delete** данной команды используется для удаления настройки внешнего адреса PPTP VPN.

Форма **show** данной команды используется для отображения настройки внешнего адреса PPTP VPN.

3.31. vpn pptp local-ip <ipv4-адрес>

Назначение внутреннего туннельного IP-адреса на сервере PPTP.

Синтаксис

```
set vpn pptp local-ip <ipv4-адрес>
delete vpn pptp local-ip
show vpn pptp local-ip
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    pptp {
        local-ip ipv4-адрес
    }
}
```

Параметры

ipv4-адрес

Обязательный. IPv4-адрес который будет назначаться PPTP VPN серверу на туннельном интерфейсе.

Значение по умолчанию

По умолчанию используется адрес 10.255.254.0.

Указания по использованию

Данная команда используется для изменения IP-адреса туннельного интерфейса на PPTP VPN сервере.

Форма **set** данной команды используется для установки IP-адреса туннельного интерфейса на PPTP VPN сервере.

Форма **delete** данной команды используется для удаления IP-адреса туннельного интерфейса на PPTP VPN сервере. После удаления используется значение по умолчанию.

Форма **show** данной команды используется для отображения IP-адреса туннельного интерфейса на PPTP VPN сервере.

3.32. vpn pptp policy [arp|ethernet|firewall|firewall-ipv6] <имя_политики>

Указание максимального размера передаваемой полезной нагрузки для PPTP VPN соединения.

Синтаксис

```
set vpn pptp policy [in|local|out] [arp|clone|clone-
ipv6|ethernet|firewall|firewall-ipv6|route| route-ipv6] <имя_политики>
delete vpn pptp policy [in|local|out] [arp|clone|clone-
ipv6|ethernet|firewall|firewall-ipv6|route| route-ipv6]
show vpn pptp policy [in|local|out] [arp|clone|clone-
ipv6|ethernet|firewall|firewall-ipv6|route| route-ipv6]
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    pptp {
        policy [in|local|out] {
            [arp|clone|clone-ipv6|ethernet|firewall|firewall-
ipv6|route|route-ipv6] имя_политики
        }
    }
}
```

Параметры

направление трафика

in: Входящий транзитный трафик, адресом назначения которого являются другие внешние узлы, а источником – PPTP VPN клиенты.

out: Исходящий транзитный трафик, адресом назначения которого являются источником PPTP VPN клиенты, а источником – другие внешние узлы.

local: Входящий локальный трафик, адресом назначения которого является PPTP VPN сервер, а источником могут быть как и PPTP VPN клиенты, так и другие внешние узлы.

тип политики

arp: Политика фильтрации ARP входящего трафика.

clone: Политика клонирования IPv4 трафика для интерфейса. (Не работает для направления **local**)

clone-ipv6: Политика клонирования IPv6 трафика для интерфейса. (Не работает для направления **local**)

ethernet: Политика фильтрации Ethernet входящего трафика. (Работает только для интерфейса, объединенного в мост)

firewall: Политика МЭ IPv4.

firewall-ipv6: Политика МЭ IPv6.

route: Политика маршрутизации IPv4 трафика для интерфейса**.** (Не работает для направления **local**)

route-ipv6: Политика маршрутизации IPv6 трафика для интерфейса. (Не работает для направления local)

имя политики

Имя существующей политики, применяемое для заданного направления.

Значение по умолчанию

Отсутствует

Указания по использованию

Используется для управления трафика, передаваемого через PPTP VPN соединение.

Форма **set** данной команды используется для задания политик трафика, передаваемого через PPTP VPN.

Форма **delete** данной команды используется для удаления политик трафика, передаваемого через PPTP VPN.

Форма **show** данной команды используется для просмотра заданных политик трафика, передаваемого через PPTP VPN.

3.33. vpn pptp wins-servers server-1 <ipv4-адрес>

Указание IP-адреса основного сервера WINS для удаленных клиентов PPTP VPN.

Синтаксис

```
set vpn pptp wins-servers server-1 <ipv4-адрес>
delete vpn pptp wins-servers server-1
show vpn pptp wins-servers server-1
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
vpn {
    pptp {
        wins-servers {
            server-1 ipv4-адрес
```

```
            }
        }
    }
```

Параметры

ipv4-адрес

IP-адрес основного сервера WINS для удаленных клиентов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания основного сервера WINS для удаленных клиентов PPTP VPN. WINS (Windows Internet Name Service) - служба сопоставления NetBIOS-имён компьютеров с IP-адресами узлов.

Форма **set** данной команды используется для указания IP-адреса основного сервера WINS.

Форма **delete** данной команды используется для удаления IP-адреса основного сервера WINS.

Форма **show** данной команды используется для отображения IP-адреса основного сервера WINS.

3.34. vpn pptp wins-servers server-2 <ipv4-адрес>

Указание IP-адреса вторичного сервера WINS для удаленных клиентов PPTP VPN.

Синтаксис

```
set vpn pptp wins-servers server-2 ipv4-адрес
delete vpn pptp wins-servers server-2
show vpn pptps wins-servers server-2
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
vpn {
    pptp {
        wins-servers {
            server-2 ipv4-адрес
        }
    }
}
```

Параметры

ipv4-адрес

IP-адрес вторичного сервера WINS для удаленных клиентов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания вторичного сервера WINS для удаленных клиентов PPTP VPN. WINS (Windows Internet Name Service) - служба сопоставления NetBIOS-имён компьютеров с IP-адресами узлов.

Форма **set** данной команды используется для указания IP-адреса вторичного сервера WINS.

Форма **delete** данной команды используется для удаления настройки IP-адреса вторичного сервера WINS.

Форма **show** данной команды используется для отображения IP-адреса вторичного сервера WINS.

3.35. interfaces pptp <pptpx>

Создание узла конфигурации клиента PPTP в системе Numa Edge.

Синтаксис

```
set interfaces pptp <pptpx>
delete interfaces pptp
show interfaces pptp
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
interfaces {
    pptp pptp0..pptp99 {
    }
}
```

Параметры

pptpx

Множественный узел. Идентификатор для определяемого интерфейса PPTP. Значение должно лежать в диапазоне от **pptp0** до **pptp99**.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для определения узла конфигурации клиента PPTP.
Форма **set** данной команды используется создания узла конфигурации клиента PPTP.
Форма **delete** данной команды используется для удаления настройки клиента PPTP.
Форма **show** данной команды используется для отображения настройки клиента PPTP.

3.36. interfaces pptp <pptpx> domain <домен>

Указание домена, который будет использоваться при аутентификации.

Синтаксис

```
set interfaces pptp pptpx domain <домен>
delete interfaces pptp domain
show interfaces pptp domain
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
interfaces {
    pptp pptp0..pptp99 {
        domain домен
    }
}
```

Параметры

pptpx

Множественный узел. Идентификатор для определяемого интерфейса PPTP. Значение должно лежать в диапазоне от **pptp0** до **pptp99**.

домен

Домен, который будет использоваться при аутентификации.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать имя домена, который используется при аутентификации.

Форма **set** данной команды используется для указания домена.

Форма **delete** данной команды используется для удаления настройки домена.

Форма **show** данной команды используется для отображения настройки.

3.37. interfaces pptp <pptpx> mppe-stateless <состояние>

Установить режим протокола MPPE.

Синтаксис

```
set interfaces pptp pptpx mppe-stateless {disable|enable}
delete interfaces pptp mppe-stateless
show interfaces pptp mppe-stateless
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
interfaces {
    pptp pptp0..pptp99 {
        mppe-stateless {disable|enable}
   }
}
```

Параметры

pptpx

Множественный узел. Идентификатор для определяемого интерфейса PPTP. Значение должно лежать в диапазоне от **pptp0** до **pptp99**.

disable

Запретить использование режима MPPE без поддержки состояний (MPPE stateless mode). По умолчанию может быть использован как режим с поддержкой состояний (MPPE stateful mode), так и режим без поддержки состояний.

enable

Разрешить использование режима MPPE без поддержки состояний (MPPE stateless mode). Используется в штатном режиме.

Значение по умолчанию

По умолчанию использование режима MPPE без поддержки состояний разрешено.

Указания по использованию

Данная команда позволяет указать используемый режим протокола MPPE (см. RFC 3078 Microsoft Point-To-Point Encryption (MPPE) Protocol).

Форма **set** данной команды позволяет включить или отключить режим использования протокола MPPE без поддержки состояний.

Форма **delete** данной команды используется для удаления текущей настройки и восстановления значения, используемого по умолчанию.

Форма **show** данной команды используется для отображения настройки режима MPPE.

3.38. interfaces pptp <pptpx> nomppe-128 <состояние>

Установить режим использования протокола MPPE с ключом длиной 128 бит.

Синтаксис

```
set interfaces pptp pptpx nomppe-128 {disable|enable}
delete interfaces pptp nomppe-128
```

```
show interfaces pptp nomppe-128
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
interfaces {
     pptp pptp0..pptp99 {
         nomppe-128 {disable|enable}
     }
}
```

Параметры

pptpx

Множественный узел. Идентификатор для определяемого интерфейса PPTP. Значение должно лежать в диапазоне от **pptp0** до **pptp99**.

disable

Разрешить использование протокола MPPE с ключом длиной 128 бит.

enable

Запретить использование протокола MPPE с ключом длиной 128 бит. Используется в штатном режиме.

Значение по умолчанию

По умолчанию использование MPPE с ключом длины 128 бит разрешено.

Указания по использованию

Данная команда позволяет установить режим использования протокола MPPE с ключом длины 128 бит.

Форма **set** данной команды позволяет запретить или разрешить использование протокола MPPE с ключами длиной 128 бит.

Форма **delete** данной команды используется для удаления текущей настройки и восстановления значения, используемого по умолчанию.

Форма **show** данной команды используется для отображения настройки.

3.39. interfaces pptp <pptpx> nomppe-40 <состояние>

Установить режим использования протокола MPPE с ключом длиной 40 бит.

Синтаксис

```
set interfaces pptp pptpx nomppe-40 {disable|enable}
delete interfaces pptp nomppe-40
show interfaces pptp nomppe-40
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
interfaces {
    pptp pptp0..pptp99 {
        nomppe-40 {disable|enable}
    }
}
```

Параметры

pptpx

Множественный узел. Идентификатор для определяемого интерфейса PPTP. Значение должно лежать в диапазоне от **pptp0** до **pptp99**.

disable

Разрешить использование протокола MPPE с ключом длиной 40 бит.

enable

Запретить использование MPPE с ключом длиной 40 бит. Используется в штатном режиме.

Значение по умолчанию

По умолчанию использование MPPE с ключом длины 40 бит разрешено.

Указания по использованию

Данная команда позволяет установить режим использования протокола MPPE с ключом длины 40 бит.

Форма **set** данной команды позволяет запретить или разрешить использование протокола MPPE с ключами длиной 40 бит.

Форма **delete** данной команды используется для удаления настройки и восстановления значения, используемого по умолчанию.

Форма **show** данной команды используется для отображения настройки.

3.40. interfaces pptp <pptpx> password <пароль>

Указание пароля, который будет использован для аутентификации.

Синтаксис

```
set interfaces pptp pptpx password <пароль>
delete interfaces pptp password
show interfaces pptp password
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
interfaces {
    pptp pptp0..pptp99 {
        password текст
    }
}
```

Параметры

pptpx

Множественный узел. Идентификатор для определяемого интерфейса PPTP. Значение должно лежать в диапазоне от **pptp0** до **pptp99**.

пароль

Пароль, который будет использован для аутентификации на сервере PPTP.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания пароля, который будет использоваться при аутентификации на сервере PPTP.

Форма **set** данной команды используется для указания пароля.

Форма **delete** данной команды используется для удаления указанного пароля.

Форма **show** данной команды используется для отображения настройки пароля.

3.41. interfaces pptp <pptpx> reconnect <состояние>

Установка режима автоматического переподключения при невозможности установления соединения, а также в случае разрыва соединения.

Синтаксис

```
set interfaces pptp pptpx reconnect {disable|enable}
delete interfaces pptp reconnect
show interfaces pptp reconnect
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
interfaces {
    pptp pptp0..pptp99 {
        reconnect {disable|enable}
    }
}
```

Параметры

pptpx

Множественный узел. Идентификатор для определяемого интерфейса PPTP. Значение должно лежать в диапазоне от **pptp0** до **pptp99**.

disable

Не устанавливать повторное подключение в случае разрыва соединения.

enable

При установке данного значения автоматически будут осуществляться попытки установить подключение после неудачной попытки установления соединения или при разрыве соединения.

Используется в штатном режиме.

Значение по умолчанию

По умолчанию установлено значение **enable**.

Указания по использованию

Данная команда позволяет указать, требуется ли устанавливать повторное подключение при разрыве соединения. По умолчанию в случае разрыва соединения, клиент PPTP производит попытку установить подключение заново.

В том случае если при фиксации конфигурации соединение установить не удалось, и при этом для параметра **reconnect** установлено значение **enable**, конфигурация будет зафиксирована, после чего будут производиться автоматические попытки подключения к серверу. При этом ограничение на количество попыток подключения отсутствует.

Форма **set** данной команды позволяет установить или отменить режим автоматического восстановления подключения при разрыве соединения.

Форма **delete** данной команды используется для удаления текущей настройки и восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки.

3.42. interfaces pptp <pptpx> refuse-eap <состояние>

Установить режим использования протокола EAP для аутентификации.

Синтаксис

```
set interfaces pptp pptpx refuse-eap {disable|enable}
delete interfaces pptp refuse-eap
show interfaces pptp refuse-eap
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
interfaces {
```

```
        pptp pptp0..pptp99 {
            refuse-eap {disable|enable}
        }
    }
```

Параметры

pptpx

Множественный узел. Идентификатор для определяемого интерфейса PPTP. Значение должно лежать в диапазоне от **pptp0** до **pptp99**.

disable

Разрешить использование протокола EAP для аутентификации. Используется в штатном режиме.

enable

Запретить использование протокола EAP для аутентификации.

Значение по умолчанию

По умолчанию использование для аутентификации протокола EAP запрещено.

Указания по использованию

Данная команда позволяет разрешить или запретить использование протокола EAP для аутентификации.

Форма **set** данной команды используется для указания режима использования протокола EAP для аутентификации.

Форма **delete** данной команды используется для удаления текущей настройки и восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки.

3.43. interfaces pptp <pptpx> remote-name <имя>

Указание имени удаленного узла, которое может использоваться для аутентификации.

Синтаксис

```
set interfaces pptp pptpx remote-name <имя>
delete interfaces pptp server
show interfaces pptp server
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
interfaces {
    pptp pptp0..pptp99 {
        remote-name имя
    }
}
```

Параметры

pptpx

Множественный узел. Идентификатор для определяемого интерфейса PPTP. Значение должно лежать в диапазоне от **pptp0** до **pptp99**.

имя

Задает имя удаленного узла, которое может использоваться для аутентификации.

Значение по умолчанию

По умолчанию используется значение pptpd.

Указания по использованию

Указывает значение имени удалённого узла, которое может использоваться для аутентификации.

Форма **set** данной команды используется для указания имени удалённого узла.

Форма **delete** данной команды используется для удаления настройки имени удалённого узла.

Форма **show** данной команды используется для отображения настройки.

3.44. interfaces pptp <pptpx> require-mppe <состояние>

Установить режим обязательного шифрования данных с использованием протокола MPPE.

Синтаксис

```
set interfaces pptp pptpx require-mppe {disable|enable}
delete interfaces pptp require-mppe
show interfaces pptp require-mppe
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
interfaces {
    pptp pptp0..pptp99 {
        require-mppe {disable|enable}
    }
}
```

Параметры

pptpx

Множественный узел. Идентификатор для определяемого интерфейса PPTP. Значение должно лежать в диапазоне от **pptp0** до **pptp99**.

disable

Отключить использование в обязательном порядке протокола MPPE для шифрования данных.

enable

Включить использование в обязательном порядке протокола MPPE для шифрования данных. Используется в штатном режиме.

Значение по умолчанию

По умолчанию требуется обязательное использование протокола MPPE для шифрования данных.

Указания по использованию

Данная команда позволяет указать, необходимо ли требовать обязательного шифрования данных с использованием протокола MPPE. Если сервер PPTP, к которому клиент производит подключение, не поддерживает шифрования данных с помощью протокола MPPE, подключение установлено не будет.

Форма **set** данной команды позволяет установить или отменить режим обязательного шифрования данных с использованием протокола MPPE.

Форма **delete** данной команды используется для удаления текущей настройки и восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки.

3.45. interfaces pptp <pptpx> server <ipv4-адрес>

Указание IP-адреса сервера PPTP.

Синтаксис

```
set interfaces pptp pptpx server <ipv4-адрес>
delete interfaces pptp server
show interfaces pptp server
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
interfaces {
    pptp pptp0..pptp99 {
        server ipv4-адрес
    }
}
```

Параметры

pptpx

Множественный узел. Идентификатор для определяемого интерфейса PPTP. Значение должно лежать в диапазоне от **pptp0** до **pptp99**.

ipv4-адрес

Обязательный. IP-адрес сервера PPTP, к которому будет осуществляться подключение.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания IP-адреса сервера PPTP.

Форма **set** данной команды используется для указания IP-адреса сервера PPTP.

Форма **delete** данной команды используется для удаления настройки IP-адреса сервера PPTP.

Форма **show** данной команды используется для отображения настройки.

3.46. interfaces pptp <pptpx> usepeerdns <состояние>

Установить режим запроса адресов серверов DNS у сервера PPTP.

Синтаксис

```
set interfaces pptp pptpx usepeerdns {disable|enable}
delete interfaces pptp usepeerdns
show interfaces pptp usepeerdns
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
interfaces {
    pptp pptp0..pptp99 {
        usepeerdns {disable|enable}
    }
}
```

Параметры

pptpx

Множественный узел. Идентификатор для определяемого интерфейса PPTP. Значение должно лежать в диапазоне от **pptp0** до **pptp99**.

disable

Не запрашивать адреса серверов DNS у сервера PPTP.

enable

Запрашивать адреса серверов DNS у сервера PPTP. Используется в штатном режиме.

Значение по умолчанию

По умолчанию установлено значение **enable**.

Указания по использованию

Данная команда позволяет указать, следует ли при подключении к серверу PPTP запрашивать адреса серверов DNS.

Форма **set** данной команды позволяет установить режим запроса адресов серверов DNS.

Форма **delete** данной команды используется для удаления текущей настройки и восстановления значения, принятого по умолчанию.

Форма **show** данной команды используется для отображения настройки.

3.47. interfaces pptp <pptpx> username <имя_пользователя>

Указание имени пользователя, которое будет использовано при аутентификации.

Синтаксис

```
set interfaces pptp pptpx username <имя_пользователя>
delete interfaces pptp username
show interfaces pptp username
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации.

```
interfaces {
    pptp pptp0..pptp99 {
        username имя_пользователя
    }
}
```

Параметры

pptpx

Множественный узел. Идентификатор для определяемого интерфейса PPTP. Значение должно лежать в диапазоне от **pptp0** до **pptp99**.

имя_пользователя

Имя пользователя, используемое при аутентификации.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда позволяет указать имя пользователя, которое будет использоваться при аутентификации.

Форма **set** данной команды используется для указания имени пользователя.

Форма **delete** данной команды используется для удаления настройки имени пользователя.

Форма **show** данной команды используется для отображения настройки.

3.48. clear vpn remote-access user <имя_пользователя>

Завершение активного сеанса указанного пользователя.

Синтаксис

```
clear vpn remote-access user имя_пользователя
```

Режим интерфейса

Эксплуатационный режим.

Ветвь конфигурации.

Отсутствует.

Параметры

имя_пользователя

Имя пользователя, активный сеанс которого требуется завершить.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для завершения всех активных сеансов указанного пользователя.

Примеры

В примере 1 приведено завершение всех активных сеансов пользователя robert.

Пример 3 - “clear vpn remote access user”: Завершение активных сеансов пользователя

```
admin@edge# clear remote-access user robert
admin@edge#
```

3.49. show vpn remote-access

Вывод сведений о текущих активных сеансах удаленного доступа VPN.

Синтаксис

```
show vpn remote-access
```

Режим интерфейса

Эксплуатационный режим.

Ветвь конфигурации.

Отсутствует.

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для вывода сведений о текущих активных сеансах VPN удаленного доступа.

Примеры

В примере 2 приведен вывод для команды **show vpn remote-access**.

Пример 4 - “show vpn remote-access”: Вывод удаленных сеансов VPN

```
admin@edge# show vpn remote-access
Active remote access VPN sessions:
User Time Proto Iface Remote IP TX pkt/byte RX pkt/byte
stig 01d02h12m PPTP ppp0 10.254.1.1 28.0K 7.7M 26.3K 2.0M shemminger
00h12m15s PPTP ppp1 10.254.1.2 85.2K 119.6M 46.6K 2.7M ancheng 15h15m33s PPTP
ppp2 10.254.1.3 73.6K 28.5M 68.3K 4.3M vpn:~#
```

Межсетевой экран Numa Edge

Руководство администратора

Мониторинг и сигнализация неисправностей оборудования

Листов 14

Санкт-Петербург
2022

СОДЕРЖАНИЕ

ИДЕНТИФИКАЦИЯ ДОКУМЕНТА

Название документа	Руководство администратора. Мониторинг и сигнализация неисправностей оборудования
Версия документа	1.0
Идентификация ОО	Межсетевой экран Numa Edge
Идентификация разработчика	ООО «НумаТех»
Ключевые слова	Межсетевой экран, МЭ, SNMP

1. МОНИТОРИНГ И СИГНАЛИЗАЦИЯ НЕИСПРАВНОСТЕЙ ОБОРУДОВАНИЯ

Для межсетевого экрана Numa Edge (далее – МЭ) имеется возможность реализовать различные сценарии по отслеживанию состояния оборудования в реальном времени с сигнализацией в случае возникновения неисправностей или превышения пороговых значений.

Исходя из практики, наиболее важными физическими компонентами, требующими отслеживания во время непрерывной работы сетевого оборудования, являются:

- процессор, для которого полезно отслеживать температуру;
- интерфейсы оборудования, для которых полезно отслеживать количество ошибок, что в свою очередь может сигнализировать о неполадках с физической коммутацией или интерфейсом непосредственно;
- устройство хранения информации, для которого также полезно отслеживать состояние и выполнять самотестирование.

В данном разделе поочередно будут рассмотрены примеры настройки мониторинга для каждого из перечисленных выше узлов.

1.1. SNMP-monitor

Большая часть примеров, рассматриваемых далее, будет опираться на настройку сервиса SNMP-monitor. Данный сервис позволяет запрашивать значения любых OID, доступных на локальном МЭ, а также сигнализировать записью в системный журнал при выполнении определенных условий, определяемых пользователем.

Для корректной работы сервиса SNMP-monitor необходимо предварительно выполнить минимальную настройку сервиса SNMP, а именно задать сообщество с именем по умолчанию и указать в качестве прослушиваемого адреса локальный адрес МЭ, как представлено на примере ниже.

Пример 1 – Настройка сервиса SNMP для дальнейшей корректной работы сервиса SNMP-monitor

Действие	**Команда**
Создание узла конфигурации сервиса SNMP. Указание сообщества SNMP	`[edit]` `admin@edge# set service snmp community public`
Указание локального адреса для прослушивания на предмет входящих запросов	`[edit]` `admin@edge# set service snmp listen-address 127.0.0.1`
Фиксация изменений	`[edit]` `admin@edge# commit`

Отображение текущей конфигурации	`[edit]`
	`admin@edge# show service snmp`
	`community public {`
	`}`
	`listen-address 127.0.0.1 {`
	`}`

После выполнения настройки SNMP можно перейти непосредственно к настройке сервиса SNMP-monitor. В качестве демонстрации работы сервиса будем выполнять запись в системный журнал в том случае, когда количество байт на входе интерфейса eth1 превышает значение 100.

Пример 2 – Запись в системный журнал при превышении количества в 100 байт на входе интерфейса eth1

Действие	**Команда**
Создание новой записи для сервиса SNMP-	`[edit]`

Действие	**Команда**
monitor	`admin@edge# set service snmp-monitor entry eth1-in`
Указание OID, который будет запрашиваться. В данном случае: `IF-MIB::ifInOctets.3` где: `IF-MIB::ifInOctets` – значение количества байт на входе интерфейса; `3` – идентификатор интерфейса eth1 в системе (можно вывести командой операционного режима show snmp mib ifmib ifIndex)	`[edit]` `admin@edge# set service snmp-monitor entry eth1-in oid IF-MIB::ifInOctets.3`
Указание типа значения, запрашиваемого OID SNMP. В данном случае `counter`. Тип `counter` указывает не абсолютное значение, а характеризует прирост в единицу времени (в данном случае в секунду) по наблюдаемому параметру	`[edit]` `admin@edge# set service snmp-monitor entry eth1-in type counter`
Указание интервала отправки сообщений в системный журнал в часах	`[edit]` `admin@edge# set service snmp-monitor entry eth1-in signal-rate 1`
Указание порогового значения, при превышении которого будет выполняться запись в системный журнал	`[edit]` `admin@edge# set service snmp-monitor entry eth1-in signal-value 100`
Фиксация изменений	`[edit]` `admin@edge# commit`

Отображение текущей конфигурации	`[edit]`
	`admin@edge# show service snmp-monitor entry eth1-in`
	`  oid IF-MIB::ifInOctets.3`
	`  signal-rate 1`
	`  signal-value 100`
	`  type counter`

Для проверки настроек можем запустить утилиту ping с внешнего адреса на указанный в примере интерфейс. По истечении пары минут в системном журнале появится соответствующая запись от приложения snmp-watcher с уровнем критичности warning о превышении порогового значения, указанного при настройке:

```
2022-07-19 16:59:01 snmp-watc daemon warnin 0 SNMP entry eth1-in больше 100
```

Примечание. Если настройки журналирования были изменены, предварительно необходимо удостовериться, что уровень критичности warning удовлетворяет условиям записи в системный журнал. В противном случае необходимо внести изменения в настройки. Более подробно с настройкой системы журнала в разделе «Регистрация событий» документа «Руководство администратора» 643.АМБН.00004-01 32 01.

1.2. Настройка мониторинга температуры процессора с записью в журнал при превышении порога

В примере производится настройка отслеживания температуры ядра 0 процессора МЭ. В случае превышения на ядре 0 процессора температуры, установленной в качестве порогового значения, будет произведена запись в системный журнал.

Пример 3 – Настройка мониторинга температуры на ядре процессора с сигнализацией в журнал

Узел конфигурации	**Действие**	**Команда**
service snmp	Создание узла конфигурации сервиса SNMP. Указание сообщества SNMP	`[edit]` `admin@edge# set service snmp community public`
	Указание локального адреса для прослушивания на предмет входящих запросов	`[edit]` `admin@edge# set service snmp listen-address 127.0.0.1`
	Фиксация изменений	`[edit]` `admin@edge# commit`

	Отображение текущей конфигурации	`[edit]`
		`admin@edge# show service snmp`
		`community public {`
		`}`
		`listen-address 127.0.0.1 {`
		`}`

service snmp-monitor	Создание новой записи для сервиса SNMP-monitor	`[edit]` `admin@edge# set service snmp-monitor entry core-0`
	Указание OID, который будет запрашиваться. Соответствует ядру 0 процессора	`[edit]` `admin@edge# set service snmp-monitor entry core-0 oid LM-SENSORS-MIB::lmTempSensorsValue.1`
	Указание типа значения запрашиваемого OID SNMP	`[edit]` `admin@edge# set service snmp-monitor entry core-0 type gauge`
	Указание интервала отправки сообщений в системный журнал в часах	`[edit]` `admin@edge# set service snmp-monitor entry core-0 signal-rate 1`
	Указание порогового значения, при превышении которого будет выполняться запись в системный журнал. По умолчанию для Intel передаются значения в величине равной 1/1000°C. Поэтому для установления порога в 80 градусов требуется указать	`[edit]` `admin@edge# set service snmp-monitor entry core-0 signal-value 80000`

Узел конфигурации	Действие	Команда
	значение 80000	
	Фиксация изменений	[edit] admin@edge# commit
	Отображение текущей конфигурации	[edit] admin@edge# show service snmp-monitor entry core-0 oid LM-SENSORS- MIB::lmTempSensorsValue.1 signal-rate 1 signal-value 80000 type gauge

В примере выше запрашивается температура только одного ядра, что является минимумом, однако она может дать представление о температуре всего процессора. При желании можно расширить количество наблюдаемых ядер, добавив новые записи в конфигурацию SNMP-monitor.

1.3. Настройка мониторинга ошибок на интерфейсе с записью в журнал при превышении порога

В примере ниже производится настройка отслеживания количества ошибок на интерфейсе eth1 МЭ. В случае превышения пороговых значений будет произведена запись в системный журнал.

Пример 4 – Настройка мониторинга ошибок при отправке трафика на интерфейсе eth1

Узел конфигурации	Действие	Команда
service snmp	Создание узла конфигурации сервиса SNMP. Указание сообщества SNMP	[edit] admin@edge# set service snmp community public
	Указание локального адреса для прослушивания на предмет входящих запросов	[edit] admin@edge# set service snmp listen-address 127.0.0.1
	Фиксация изменений	[edit] admin@edge# commit

	Отображение текущей конфигурации	[edit]
		admin@edge# show service snmp
		community public {
		}
		listen-address 127.0.0.1 {
		}

service snmp-monitor	Создание новой записи для сервиса SNMP-monitor	[edit] admin@edge# set service snmp- monitor entry eth1-in-err
	Указание OID, который будет запрашиваться.	[edit] admin@edge# set service snmp-

Узел конфигурации	Действие	Команда
	Соответствует количеству пакетов на входе интерфейса eth1, содержащих ошибки, предотвращающие возможность передачи пакета далее в обработку	`monitor entry eth1-in-err oid IF-MIB::ifInErrors.3`
	Указание типа значения запрашиваемого OID SNMP	`[edit]` `admin@edge# set service snmp-monitor entry eth1-in-err type counter`
	Указание интервала отправки сообщений в системный журнал в часах	`[edit]` `admin@edge# set service snmp-monitor entry eth1-in-err signal-rate 1`
	Указание порогового значения, при превышении которого будет выполняться запись в системный журнал	`[edit]` `admin@edge# set service snmp-monitor entry eth1-in-err signal-value 40`
	Создание новой записи для сервиса SNMP-monitor	`[edit]` `admin@edge# set service snmp-monitor entry eth1-out-err`
	Указание OID, который будет запрашиваться. Соответствует количеству исходящих пакетов на интерфейса eth1, содержащих ошибки, предотвращающие возможность передачи пакета далее	`[edit]` `admin@edge# set service snmp-monitor entry eth1-out-err oid IF-MIB::ifOutErrors.3`
	Указание типа значения запрашиваемого OID SNMP	`[edit]` `admin@edge# set service snmp-monitor entry eth1-out-err type counter`
	Указание интервала отправки сообщений в системный журнал в часах	`[edit]` `admin@edge# set service snmp-monitor entry eth1-out-err signal-rate 1`
	Указание порогового значения, при превышении которого будет выполняться запись в системный журнал	`[edit]` `admin@edge# set service snmp-monitor entry eth1-out-err signal-value 40`
	Фиксация изменений	`[edit]` `admin@edge# commit`
	Отображение текущей конфигурации	`[edit]` `admin@edge# show service snmp-monitor entry`

Узел конфигурации	Действие	Команда

		eth1-in-err {
		oid IF-MIB::ifInErrors.3
		signal-rate 1
		signal-value 40
		type counter
		}
		eth1-out-err {
		oid IF-MIB::ifOutErrors.3
		signal-rate 1
		signal-value 40
		type counter
		}

Таким образом, при превышении порогового значения по приросту количества ошибок в одном из направлений на интерфейсе eth1 будет осуществлена запись в системный журнал. Для остальных интерфейсов настройка выполняется аналогичным образом.

1.4. Мониторинг состояния устройства хранения информации

Контроль за состоянием устройства хранения информации в МЭ отвечает сервис smartd. Данный сервис сконфигурирован для работы в полностью автоматическом режиме. Таким образом, со стороны пользователя нет необходимости предварительно выполнять какие-либо настройки.

В случае обнаружения неисправностей с носителем информации во время работы устройства, сервис будет сигнализировать соответствующими записями в системный журнал.

Пример 5 – Запись в системном журнале о неисправности носителя информации

```
2022-07-20 14:14:00 smartd    daemon crit   0 Device: /dev/sda [SAT], 16 Currently unreadable (pending) sectors
2022-07-20 14:44:00 smartd    daemon crit   0 Device: /dev/sda [SAT], 16 Currently unreadable (pending) sectors
```

По умолчанию интервал отправки сообщений составляет 30 минут.

1.5. Команды сервиса SNMP-monitor

Команды настройки	
service snmp-monitor	Включение сервиса локального мониторинга показателей, доступных посредством SNMP
service snmp-monitor entry <запись>	Создание новой записи в сервисе SNMP-monitor
service snmp-monitor entry <запись> oid <идентификатор>	Указание SNMP OID для записи в сервисе SNMP-monitor
service snmp-monitor entry <запись> signal-rate <интервал>	Указание временного интервала для сигнализации в системный журнал для записи в сервисе SNMP-monitor
service snmp-monitor entry <запись>	Указание порогового значения, при превышении которого

Команды настройки	
signal-value <значение>	будет выполнена сигнализация в системный журнал
service snmp-monitor entry <запись> type <тип>	Указание используемого типа данных для интерпретации значений наблюдаемого SNMP OID
Эксплуатационные команды	
service snmp-monitor show <запись>	Просмотр значений наблюдаемого SNMP OID для указанной записи сервиса SNMP-monitor за период времени

1.5.1. service snmp-monitor

Включение сервиса локального мониторинга показателей, доступных посредством SNMP.

Синтаксис

```
set service snmp-monitor
delete service snmp-monitor
show service snmp-monitor
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   snmp-monitor {
   }
}
```

Параметры

Отсутствуют.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для включения локального мониторинга показателей посредством SNMP, позволяет указать запрашиваемый OID и его тип, а также параметры по сигнализации в системный журнал.

Форма **set** данной команды используется для включения локального мониторинга SNMP.

Форма **delete** данной команды используется для удаления конфигурации SNMP-monitor.

Форма **show** данной команды используется для отображения конфигурации SNMP-monitor.

1.5.2. service snmp-monitor entry <запись>

Создание новой записи в сервисе SNMP-monitor.

Синтаксис

```
set service snmp-monitor entry <запись>
delete service snmp-monitor entry <запись>
show service snmp-monitor entry <запись>
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
```

```
        snmp-monitor {
            entry запись {
            }
        }
    }
```

Параметры

запись

Множественный узел. Запись SNMP-monitor. Содержит один SNMP OID и параметры сигнализации в системный журнал.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для создания новой записи в сервисе SNMP-monitor.

Форма **set** данной команды используется для создания записи в конфигурации сервиса SNMP-monitor.

Форма **delete** данной команды используется для удаления записи из конфигурации сервиса SNMP-monitor.

Форма **show** данной команды используется для отображения параметров записи.

1.5.3. service snmp-monitor entry <запись> oid <идентификатор>

Указание SNMP OID для записи в сервисе SNMP-monitor.

Синтаксис

```
set service snmp-monitor entry <запись> oid <идентификатор>
delete service snmp-monitor entry <запись> oid [<идентификатор>]
show service snmp-monitor entry <запись> oid
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
    snmp-monitor {
        entry запись {
            oid идентификатор
        }
    }
}
```

Параметры

запись

Множественный узел. Запись SNMP-monitor.

идентификатор

SNMP OID. Запрашиваемая характеристика, которую ставим под наблюдение посредством сервиса.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания наблюдаемого SNMP OID в указанной записи сервиса SNMP-monitor.

Форма **set** данной команды используется для указания SNMP OID.

Форма **delete** данной команды используется для удаления SNMP OID из указанной записи.

Форма **show** данной команды используется для отображения SNMP OID.

1.5.4. service snmp-monitor entry <запись> signal-rate <интервал>

Указание временного интервала для сигнализации в системный журнал для записи в сервисе SNMP-monitor.

Синтаксис

```
set service snmp-monitor entry <запись> signal-rate <интервал>
delete service snmp-monitor entry <запись> signal-rate
[<интервал>]
show service snmp-monitor entry <запись> signal-rate
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   snmp-monitor {
      entry запись {
         signal-rate интервал
      }
   }
}
```

Параметры

запись

Множественный узел. Запись SNMP-monitor.

интервал

Временной интервал для сигнализации в системный журнал. Указывается количество часов. Сигнализация будет выполняться не чаще одного раза в указанное количество часов.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания временного интервала для записи сервиса SNMP-monitor.

Форма **set** данной команды используется для указания временного интервала.

Форма **delete** данной команды используется для удаления временного интервала из указанной записи.

Форма **show** данной команды используется для отображения временного интервала.

1.5.5. service snmp-monitor entry <запись> signal-value <значение>

Указание порогового значения, при превышении которого будет выполнена сигнализация в системный журнал.

Синтаксис

```
set service snmp-monitor entry <запись> signal-value <значение>
delete service snmp-monitor entry <запись> signal-value
[<значение>]
show service snmp-monitor entry <запись> signal-value
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   snmp-monitor {
      entry запись {
         signal-value значение
      }
   }
}
```

Параметры

запись

Множественный узел. Запись SNMP-monitor.

значение

Пороговое значение для сигнализации в системный журнал. Для корректной настройки необходимо иметь представление о том, в каком формате передается тот или иной SNMP OID.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания порогового значения для записи сервиса SNMP-monitor.

Форма **set** данной команды используется для указания порогового значения.

Форма **delete** данной команды используется для удаления порогового значения из указанной записи.

Форма **show** данной команды используется для отображения порогового значения.

1.5.6. service snmp-monitor entry <запись> type <тип>

Указание используемого типа данных для интерпретации и хранения значений наблюдаемого SNMP OID.

Синтаксис

```
set service snmp-monitor entry <запись> type <тип>
delete service snmp-monitor entry <запись> type [<тип>]
show service snmp-monitor entry <запись> type
```

Режим интерфейса

Режим настройки.

Ветвь конфигурации

```
service {
   snmp-monitor {
      entry запись {
         type тип
      }
   }
}
```

Параметры

запись

Множественный узел. Запись SNMP-monitor.

тип

Используемый тип данных. Возможные значения:

- gauge: значения наблюдаемого SNMP OID обрабатываются как абсолютные. Используется в том случае, когда SNMP OID имеет тип gauge и передает абсолютные значения. В качестве примера применимо для показаний датчиков температуры;
- counter: значения наблюдаемого SNMP OID обрабатываются как показания счетчика. Используется в том случае, когда SNMP OID имеет тип counter и передает прирост показателя в единицу времени. В качестве примера применимо для показаний ошибок на интерфейсе.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для указания типа данных для записи сервиса SNMP-monitor.

Форма **set** данной команды используется для указания типа данных.

Форма **delete** данной команды используется для удаления типа данных из указанной записи.

Форма **show** данной команды используется для отображения типа данных.

1.5.7. service snmp-monitor show <запись>

Просмотр значений наблюдаемого SNMP OID для указанной записи сервиса SNMP-monitor за период времени.

Синтаксис

```
service snmp-monitor show <запись> [avg|max|min from <время> [to <время>] [step <шаг>]]
```

Режим интерфейса

Эксплуатационный режим.

Параметры

запись

Запись SNMP-monitor.

avg

Показ усредненных данных для указанного объекта.

max

Показ максимальных значений для указанного объекта.

min

Показ минимальных значений для указанного объекта.

время

Задать временной отрезок, за который выводить данные. Используется формат отрицательных чисел с приставками day, h, min, а также слово now. Например -2h, -5min. Конструкция from -1h to now выведет данные за последний час.

шаг

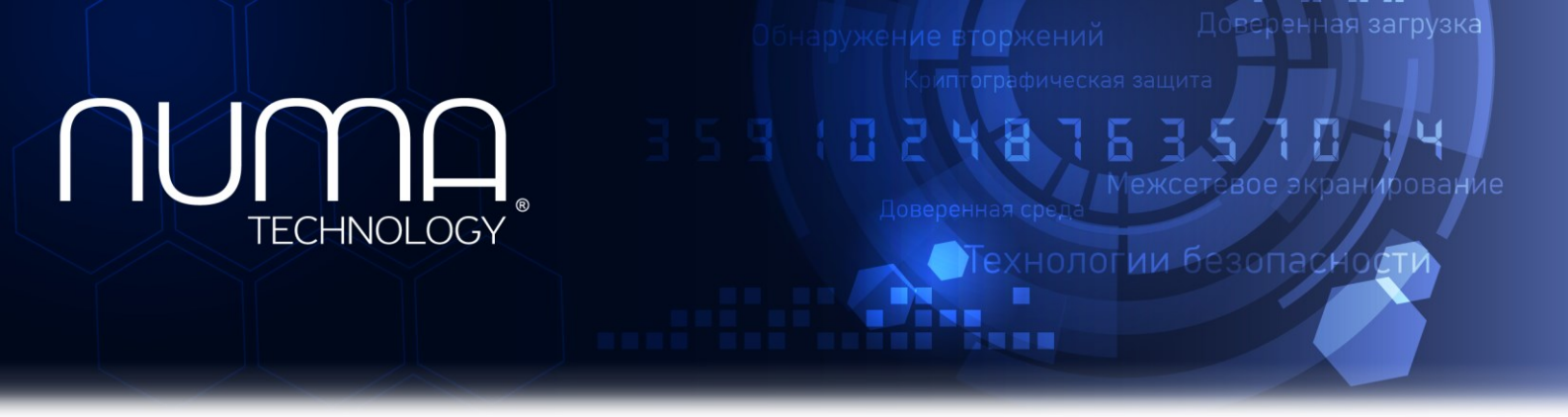
Указать периодичность при выводе значений на определенном ранее временном отрезке. Используется формат положительных чисел приставками day, h, min. Например, 20min. Конструкция from -1h to now step 20min выведет три записи с интервалом 20 минут за последний час. Минимальный шаг составляет 1min.

Значение по умолчанию

Отсутствует.

Указания по использованию

Данная команда используется для просмотра показаний для указанной записи SNMP-monitor за временной интервал.



Программно-аппаратный комплекс Numa Edge
Использование Numa Edge для защиты от DDoS на границе сети
Листов 15

Санкт-Петербург
2020

СОДЕРЖАНИЕ

ИДЕНТИФИКАЦИЯ ДОКУМЕНТА

Название документа	Использование Numa Edge для защиты от DDoS на границе сети
Версия документа	Версия 1.0
Идентификация ОО	Межсетевой экран Numa Edge
Идентификация разработчика	ООО «НумаТех»
Ключевые слова	Межсетевой экран, МЭ, DDoS

1. ОСОБЕННОСТИ ФОРМАТИРОВАНИЯ ДОКУМЕНТА

В данном документе используются следующие особенности форматирования:

- примеры параметров команд, используемых в конфигурации, но используемые в тесте для примеров выделены моноширинным шрифтом;
- специальные термины, впервые используемые в тексте обозначены курсивным шрифтом;
- примеры конфигурации и листинги команды выделены в отдельные блоки без специальных пометок:

```
листинг команды
```

- важная информация, влияющая на особенности конфигурации обозначена специальным блоком с пометкой **ВАЖНО!**:

ВАЖНО!

- примечания и некоторые особенности поведения системы обозначены специальным блоком с пометкой **ПРИМЕЧАНИЕ!**:

ПРИМЕЧАНИЕ!

- общие замечания выделены специальным блоком с пометкой **ИНФОРМАЦИЯ:**

ИНФОРМАЦИЯ:

2. ВВЕДЕНИЕ

Ключевым понятием в работе межсетевого экрана является соотнесение проходящих IP пакетов, имеющих одинаковые адреса и порты отправителя и получателя, в общий поток трафика, называемый соединением. Отслеживание состояния соединений позволяет существенно упростить настройку межсетевого экрана, а также увеличить его быстродействие. Вместо того чтобы применять правила фильтрации для всего трафика, возможно ограничивать каким-либо образом только новые соединения и разрешать уже установленные. Практически классическим методом применения данного способа является разрешение установления новых соединений только из внутренней сети, в то время как из внешней сети разрешается только прохождение пакетов для уже установленного соединения. Однако, возникают сложности если из внешней сети возможно также установление новых соединений.

В этом сценарии использования будет рассмотрен вопрос настройки правил фильтрации и межсетевого экранирования на устройстве ПАК Numa Edge FW (далее – *устройство*) для защиты сервера, к которому необходимо организовать удаленное подключение из внешней сети. В качестве примера будет рассматриваться фильтрация входящего трафика к внутреннему Веб-серверу (далее - *сервер*) компании. Для проходящего через МЭ трафика будут выполняться различные проверки на предмет корректности. Весь трафик, помеченный как некорректный, будет заблокирован и не будет поступать на сервер. Данные действия помогут обезопасить сервер от атак типа отказ в обслуживании. Отдельно стоит обратить внимание, что в сценарии описываются примеры защиты на сетевом и транспортном уровне модели TCP/IP.

Настоятельно рекомендуется пред изучением данного сценария ознакомиться с документом «643.АМБН.00004-01 32 01 Руководство администратора» (далее - *РА*), поскольку основное внимание сфокусировано на особенностях конфигурации сложных правил фильтрации и взаимодействия различных политик межсетевого экранирования между собой.

3. ИСХОДНЫЕ ДАННЫЕ

3.1. Оборудование

- Устройство ПАК Numa Edge FW используется для на границе между внешней и внутренней сетью. На устройстве происходит фильтрация и журналирование паразитного трафика, осуществляется обеспечение доступа и контроль поступающего трафика к серверу расположенному внутри защищаемой сети.
- Конфигурация Web-сервера в данном примере не рассматривается, но считается что к нему будут подключаться клиенты, используя порты 443/TCP и 80/TCP.

ПРИМЕЧАНИЕ! Функционал устройства ПАК Numa Edge FW полностью аналогичен функционалу ПАК Numa Edge VPN в части межсетевого экранирования. Поэтому возможен сценарий использования, при котором устройство ПАК Numa Edge VPN является и шлюзом удаленных подключений, и обеспечивает функционал межсетевого экрана на границе сети. Однако, хорошей практикой является разнесение этих функциональных обязанностей между различными устройствами.

3.2. Схема подключения

Устройство устанавливается на границе между внутренней и внешней сетью. Интерфейс *eth1* подключается к внешней сети и имеет IP-адрес *1.2.3.4/24*. На этом интерфейсе настраивается политика межсетевого экранирования для входящего трафика, отправляемого на внутренний Веб-сервер из внешней сети. Интерфейс *eth2 подключен* к внутренней сети и имеет адрес *192.168.10.254/24*. IP-адрес Веб-сервера - *192.168.10.200/24*. Для перенаправления трафика, поступающего из внешней сети, на Веб-сервер применяется трансляция адреса отправителя (DNAT). Общая схема обработки входящего трафика на устройстве представлена на рисунке 1.

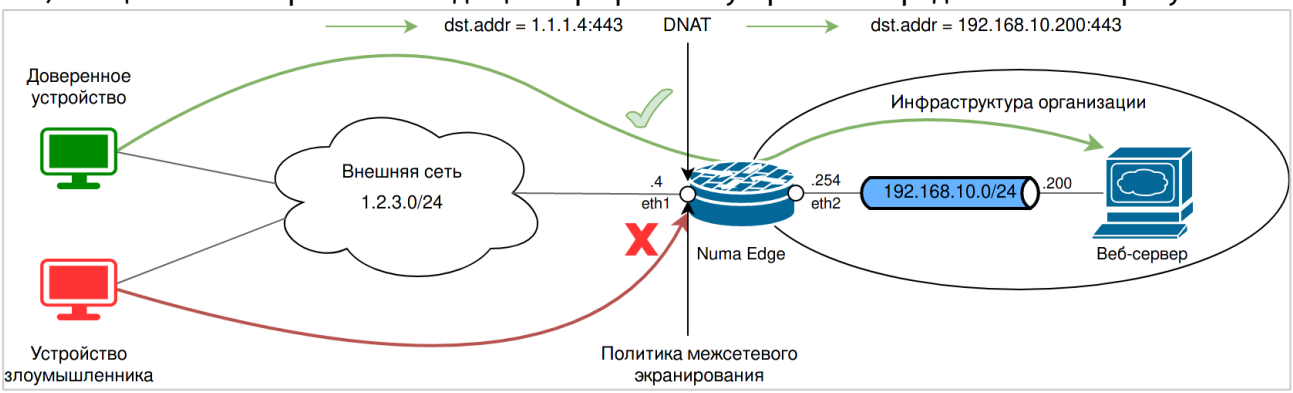


Рисунок 1 – Общая схема обработки входящего трафика на устройстве

ИНФОРМАЦИЯ: согласно RFC 6890 для описания в документации внешних подсетей необходимо использовать IP-адреса из следующих диапазонов: 192.0.2.0/24 (TEST-NET-1), 198.51.100.0/24 (TEST-NET-2) и 203.0.113.0/24 (TEST-NET-3). Однако, поскольку эти же диапазоны запрещены к использованию, они будут описаны в правилах фильтрации для немаршрутизируемых подсетей.

4. ОПИСАНИЕ ПРИНЦИПА РАБОТЫ ПОЛИТИК МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ

Настройка межсетевого экрана состоит из трех основных компонент:

- Описание паттернов трафика в политике фильтрации;
- Указание правил действия для трафика, попадающего под указанный фильтр в политике МЭ;
- Определение точки входа/выхода трафика и применение политики МЭ.

Под паттерном трафика понимаются такие значения полей пакетов сетевого уровня и выше (согласно модели TCP/IP), по которым возможно его соотнесение с определенным правилом фильтрации. В этом примере рассматривается особенность работы межсетевого экрана для протокола IPv4.

На рисунке 2 приведена иерархическая схема работы политик МЭ. Каждая политика фильтрации может состоять из одного или нескольких правил фильтрации. Данные правила только маркируют трафик внутри системы, никак его не изменяя. Каждая политика фильтрации добавляется к правилу фильтрации, к которому применяется определенное действие, например, разрешение или запрет. Набор из одного или нескольких правил МЭ представляет собой политику МЭ, для которой указывается место применения. В этом примере настраивается политика МЭ для входящего трафика из внешней сети. Поэтому, согласно рисунку 1, политика будет применяться на интерфейсе *eht1* для направления *in*.

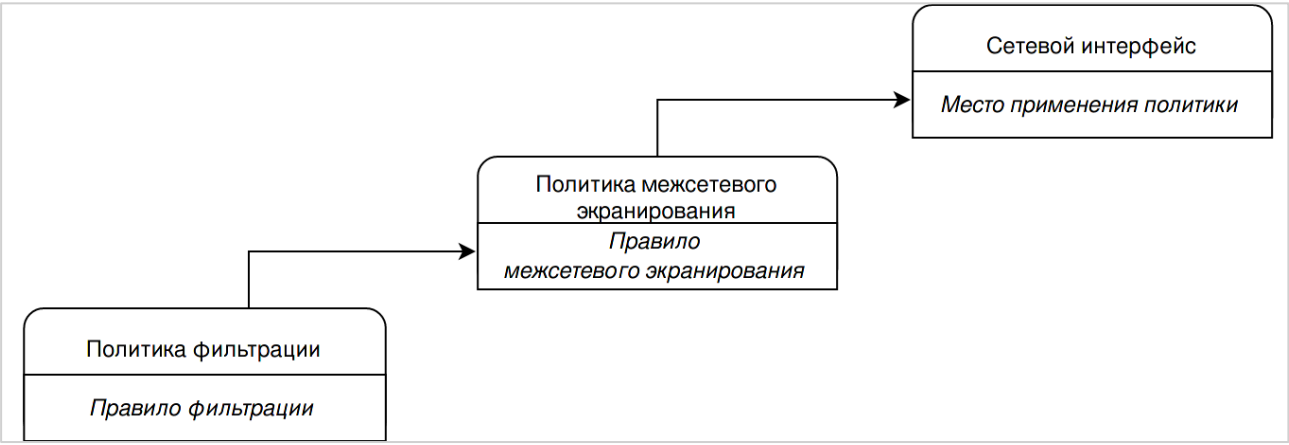


Рисунок 2 – Иерархическая схема работы политик МЭ

5. КОНФИГУРАЦИЯ УСТРОЙСТВА

5.1. Настройка интерфейсов

Для настройки устройства необходимо перейти в конфигурационный режим с помощью команды:

```
admin@edge:~$ configure
[edit]
admin@edge#
```

После перехода в конфигурационный режим изменяется интерфейс приглашения для ввода, как указано на листинге выше. Все последующие примеры приведены без отображения приглашения.

Первоначально настраиваются IP-адреса на сетевых интерфейсах, согласно схеме на рисунке 1.

```
set interfaces ethernet eth1 description "Внешний интерфейс"
set interfaces ethernet eth1 address '1.2.3.4/24'
```

```
set interfaces ethernet eth2 description "Внутренний интерфейс"
set interfaces ethernet eth2 address '192.168.10.100/24'
```

Далее, необходимо обеспечить перенаправление HTTP и HTTPS трафика на сервер. Для этого настраивается правило с номером 10 для трансляции сетевых адресов назначения. В нем указывается перенаправление трафика для пакетов с адресом назначения *1.2.3.4 и* портами назначения *80 и 443,* для протокола *TCP* на адрес *192.168.10.200*. В этом примере порты назначения после трансляции не изменяются. Для правил трансляции используется литеральная запись портов назначения, но возможно и использование числовой записи.

```
set service nat ipv4 rule 10 description "Трансляция входящего HTTP/HTTPS трафика на сервер"
set service nat ipv4 rule 10 destination address '1.2.3.4'
set service nat ipv4 rule 10 destination port http,https
set service nat ipv4 rule 10 inbound-interface 'eth1'
set service nat ipv4 rule 10 inside-address address '192.168.10.200'
set service nat ipv4 rule 10 protocol 'tcp'
set service nat ipv4 rule 10 type 'destination'
```

Правило с номером 20 перенаправляет ответы сервера во внешнюю сеть, которое настраивается аналогичным образом.

```
      set service nat ipv4 rule 10 description "Трансляция
исходящего HTTP/HTTPS трафика от сервера"
      set service nat ipv4 rule 20 outbound-interface 'eth1'
      set service nat ipv4 rule 20 outside-address address '1.2.3.4'
      set service nat ipv4 rule 20 protocol 'tcp'
      set service nat ipv4 rule 20 source address '192.168.10.200'
      set service nat ipv4 rule 20 source port 'http,https'
      set service nat ipv4 rule 20 type 'source'
```

После ввода данных настроек для их применения используется команда:

```
commit
```

Для сохранения настроек используется команда:

```
save
```

5.2. Настройка политик фильтрации

Далее производится настройка политик фильтрации для входящего трафика. Особенностью системы конфигурации устройства является возможность настройки политик фильтрации, для последующего их применения в различных правилах политик МЭ. Таким образом, большинство политик, созданных в этом примере, могут применяться и для фильтрации входящего трафика для направления *local* – политики МЭ для входящего трафика на устройство, которая не рассматривается в данном сценарии.

В политиках фильтрации трафика производится обнаружение паттернов трафика, часто используемого для реализации различных видов атак как на оборудование внутри локальной сети, так и на сам межсетевой экран, расположенный на границе. Будет рассмотрена настройка устройства для защиты от следующих методов и типов атак:

- некорректные адреса источника отправителя;
- отправка пакетов с некорректными параметрами;
- различные атаки, направленные на протокол TCP.

5.2.1. Некорректные адреса источника пакетов

Создается группа адресов, указывающие на список подсетей, которые не должны использоваться в Интернете. Список этих подсетей приведен в RFC 5375 и 6890.

```
      set groups address-group Bogons description
"Немаршрутизируемые подсети"
      set groups address-group Bogons address '0.0.0.0/8'
      set groups address-group Bogons address '10.0.0.0/8'
      set groups address-group Bogons address '100.64.0.0/10'
      set groups address-group Bogons address '127.0.0.0/8'
      set groups address-group Bogons address '169.254.0.0/16'
      set groups address-group Bogons address '172.16.0.0/12'
      set groups address-group Bogons address '192.0.0.0/24'
      set groups address-group Bogons address '192.0.2.0/24'
      set groups address-group Bogons address '192.88.99.0/24'
      set groups address-group Bogons address '192.168.0.0/16'
      set groups address-group Bogons address '198.18.0.0/15'
      set groups address-group Bogons address '198.51.100.0/24'
      set groups address-group Bogons address '203.0.113.0/24'
      set groups address-group Bogons address '224.0.0.0/3'
```

ИНФОРМАЦИЯ: диапазон '224.0.0.0/3' включает в себя подсеть '224.0.0.0/4', описанную в RFC 1122, определенную для использования в качестве Multicast адресов, а также подсеть 240.0.0.0/4 – зарезервированную IANA и включающую в себя адрес 255.255.255.255 – Broadcast адрес.

Данный список подсетей не должен использоваться в качестве источника пакетов из внешней сети, поэтому создается политика фильтрации, в которой в качестве адреса источника указывается ранее созданная группа адресов.

```
      set filter Bogons-on-WAN description 'Немаршрутизируемые сети
не должны быть источником пакетов во внешней сети'
      set filter Bogons-on-WAN rule 10 source address-group 'Bogons'
```

5.2.2. Некорректные флаги TCP

Флаги TCP, содержащиеся в заголовке пакета бывают 6 различных типов:

- **SYN** – Синхронизация порядковых номеров.
- **ACK** – Флаг пакета, содержащего уведомление о получении.
- **FIN** – Флаг окончания передачи со стороны отправителя.
- **RTS** – Сброс соединения.
- **URG** – Флаг срочности.
- **PSH** – Флаг форсированной отправки сегмента (запрос операции PUSH).

Подробности установления соединения и использования различных флагов описаны в RFC 793, а также на странице 23 указана диаграмма состояния соединений, в которой описаны используемые флаги для перехода между состояниями.

Следующая политика фильтрации описывает сочетание TCP флагов, которые не используются в штатном режиме работы протокола. Некорректные TCP флаги используются для различных реализаций атак типа TCP Null Attack, Xmas attack и т.д

Для каждого правила фильтрации указывается протокол TCP, и описываются флаги по следующем принципу:

- если указан тип флага: **FIN** – данный флаг должен быть установлен (значение бита флага в пакете равно 1);

- если указан тип флага с восклицательным знаком: **!FIN** – данный флаг не должен быть установлен (значение бита флага в пакете равно 0);
- если флаг не указан – данный флаг не проверяется правилом и может иметь любое значение.
- для описания всех флагов со значением 1 указывается флаг **ALL** и **!ALL** для всех флагов со значением 0.

```
      set filter Bogus-TCP-Flags description 'Некорректные TCP
флаги, которые не должны обрабатываться'
      set filter Bogus-TCP-Flags rule 10 protocol 'tcp'
      set filter Bogus-TCP-Flags rule 10 tcp flags 'FIN,!ACK'
      set filter Bogus-TCP-Flags rule 20 protocol 'tcp'
      set filter Bogus-TCP-Flags rule 20 tcp flags 'FIN,SYN'
      set filter Bogus-TCP-Flags rule 30 protocol 'tcp'
      set filter Bogus-TCP-Flags rule 30 tcp flags 'SYN,RST'
      set filter Bogus-TCP-Flags rule 40 protocol 'tcp'
      set filter Bogus-TCP-Flags rule 40 tcp flags 'FIN,RST'
      set filter Bogus-TCP-Flags rule 50 protocol 'tcp'
      set filter Bogus-TCP-Flags rule 50 tcp flags 'URG,!ACK'
      set filter Bogus-TCP-Flags rule 60 protocol 'tcp'
      set filter Bogus-TCP-Flags rule 60 tcp flags 'PSH,!ACK'
      set filter Bogus-TCP-Flags rule 70 protocol 'tcp'
      set filter Bogus-TCP-Flags rule 70 tcp flags '!ALL'
      set filter Bogus-TCP-Flags rule 80 protocol 'tcp'
      set filter Bogus-TCP-Flags rule 80 tcp flags 'ALL'
      set filter Bogus-TCP-Flags rule 90 protocol 'tcp'
      set   filter   Bogus-TCP-Flags   rule   90   tcp   flags
'FIN,!SYN,!RST,PSH,!ACK,URG'
      set filter Bogus-TCP-Flags rule 100 protocol 'tcp'
      set   filter   Bogus-TCP-Flags   rule   100   tcp   flags
'FIN,SYN,!RST,PSH,!ACK,URG'
      set filter Bogus-TCP-Flags rule 110 protocol 'tcp'
      set   filter   Bogus-TCP-Flags   rule   110   tcp   flags
'FIN,SYN,RST,!PSH,ACK,URG'
```

5.2.3. Фальшивые TCP Reset

Пакеты TCP с установленным флагом RST сами по себе являются корректными, однако их большое количество, отправляемого с одного адреса может свидетельствовать об атаке типа TCP Reset. Данная атака относится к классу атак посредника, когда посторонний наблюдатель прослушивает трафик и генерирует пакеты с корректными параметрами, такими как адреса и порт отправителя и получателя, а также указывая правильный номер TCP последовательности для сброса установленных соединений путем отправки пакета с флагом RST.

Для нейтрализации данного типа атак применяется ограничение количества получаемых TCP RST пакетов. В этом примере разрешается прохождение не более 2 таких пакетов в секунду от одного адреса отправителя.

Данная политика фильтрации состоит из двух правил. В правиле 10 используется параметр *exclude*, которое работает следующим образом: **Если от отправителя приходит один или два TCP пакета в секунду с флагом RST - исключить пакет из правила фильтрации.** Зачем исключать пакет из правила фильтрации? Все описанные ранее правила фильтрации описывали некорректные пакеты, для которых затем будет применено действие *drop* в соответствующем правиле МЭ. Если для этой политики фильтрации действие правила МЭ будет *accept*, то данные пакеты не будут

обработаны последующими правилами фильтрации. Таким образом для организации цепочки проверок различными политиками фильтрации – корректные пакеты исключаются из политики фильтрации. **Для блокировки 3 и более пакетов в секунду создается правило 20 – описывающее TCP пакет с флагом RST, для которого будет применено действие drop в соответствующей политике МЭ.**

```
      set filter TCP-Reset description 'Большое количество TCP
пакетов с флагом RST'
      set filter TCP-Reset rule 10 'exclude'
      set filter TCP-Reset rule 10 limit connection-rate source-
mask 32
      set filter TCP-Reset rule 10 limit connection-rate group-by
'source-address'
      set filter TCP-Reset rule 10 limit connection-rate upto '2'
      set filter TCP-Reset rule 10 protocol 'tcp'
      set filter TCP-Reset rule 10 tcp flags 'RST'
      set filter TCP-Reset rule 20 protocol 'tcp'
      set filter TCP-Reset rule 20 tcp flags 'RST'
```

5.2.4. Некорректные значения MSS

В статье на сайте APNIC (Азиатско-Тихоокеанский сетевой информационный центр) под названием "TCP MSS values – what's changed?" (Значения TCP MSS - что изменилось?) после обнаруженных уязвимостей CVE-2019-11477, 11478 и 11479 связанных с некорректной обработкой малых значений MSS в TCP пакетах рекомендуется блокировать пакеты со значением меньше 500. Для этого создается правило фильтрации, описывающее данный диапазон значений.

```
      set filter Uncommon-MSS description 'Некорректное значение TCP
MSS'
      set filter Uncommon-MSS rule 10 protocol 'tcp'
      set filter Uncommon-MSS rule 10 tcp mss '0-500'
```

5.2.5. Новые TCP соединения с некорректным флагом

Согласно RFC 793, стр.23 TCP соединения должны начитаться с отправки пакета с флагом SYN. Поэтому создается фильтр, в который попадают все пакеты с флагом, отличным от SYN и только что пришедшие на устройство.

```
      set filter New-not-SYN rule 10 protocol 'tcp'
      set filter New-not-SYN rule 10 state new 'enable'
      set filter New-not-SYN rule 10 tcp flags '!SYN'
      set filter New-not-SYN description 'Новые TCP пакеты без флага
SYN'
```

Необходимо иметь в виду, что состояние соединения в МЭ и состояние TCP-сессии между клиентом и сервером имеют принципиальные различия. Уникальность каждого пакета определяется путем соотнесения адресов и портов источника и назначения с уже существующими табличными данными. Таким образом первому поступающему в МЭ TCP пакету (отправленного от клиента к серверу) с флагом SYN будет присвоено состояние NEW. Ответный же пакет, содержащий флаг SYN/ACK, проходящий через МЭ переведет состояние соединения в ESTABLISHED. При этом сервер ожидает пакет от клиента с флагом ACK, для подтверждения установления соединения и перевода в состояние ESTABLISHED TCP сессии. Поэтому для перевода состояния соединения в МЭ с

NEW на ESTABLISHED требуется прохождение двух пакетов от клиента к серверу, в то время как для установления TCP соединения между ними требуется 3 пакета.

5.2.6. Ограничение новых соединений от одного адреса источника

Принцип работы политики *Sync-flood* в целом схож по логике работы с политикой *TCP-Reset*. Он основан на предположении того, что с определенного адреса источника не должно открываться большое количество TCP соединений. В этом примере используется ограничение в 20 пакетов в секунду, но данный параметр должен подбираться индивидуально, в зависимости от конфигурации сервера и ожидаемого количества подключений. Фильтр работает следующим образом: **Если с определенного адреса источника приходит 20 пакетов в секунду или *меньше* - исключить из политики фильтрации.** Другим способом реализации подобной задачи, является использование параметра *above* – который ограничивает *максимальную* скорость прохождения пакетов. При использовании параметра *above* – правило фильтрации должно настраиваться без параметра *exclude*.

```
      set filter Sync-flood description 'Ограничение новых
соединений от одного адреса источника'
      set filter Sync-flood rule 10 'exclude'
      set filter Sync-flood rule 10 limit connection-rate source-
mask 32
      set filter Sync-flood rule 10 limit connection-rate group-by
'source-address'
      set filter Sync-flood rule 10 limit connection-rate upto '20'
      set filter Sync-flood rule 10 protocol 'tcp'
      set filter Sync-flood rule 10 state new 'enable'
```

Правило 20 является опциональным и описывает регистрацию в системном журнале 5 пакетов в секунду, которые были исключены из предыдущего правила. Поскольку атаки типа TCP Sync flood обычно состоят из огромного количества пакетов в секунду – нет смысла регистрировать все отбрасываемые пакеты. Использование журналирования в правиле фильтрации, а не в политике МЭ объясняется как раз возможностью указания ограничения записей в системный журнал за единицу времени.

```
      set filter Sync-flood rule 20 protocol 'tcp'
      set filter Sync-flood rule 20 state new 'enable'
      set filter Sync-flood rule 20 limit packet-rate rate '5'
      set filter Sync-flood rule 20 log 'enable'
```

Правило фильтрации 30 используется для последующей блокировки в политике МЭ.

```
      set filter Sync-flood rule 30 protocol 'tcp'
      set filter Sync-flood rule 30 state new 'enable'
```

Политику фильтрации, описанную в этом примере также возможно использовать для протоколов UDP или ICMP в случае необходимости изменив соответствующий параметр *protocol* в правилах фильтрации.

5.2.7. Некорректное состояние соединения

Если состояние соединения невозможно классифицировать, оно помечается как некорректное и связанные с ним пакеты должны быть заблокированы.

```
      set filter State-Invalid rule 10 state invalid 'enable'
      set filter State-Invalid description 'Пакеты с некорректным
состоянием'
```

5.2.8. Открытие портов HTTP и HTTPS.

Последнее правило фильтрации используется для явного разрешения прохождения пакетов на сервер для протоколов HTTP и HTTPS.

```
      set filter WEB-server rule 10 destination port http,https
      set filter WEB-server rule 10 protocol tcp
```

5.3. Настройка политики межсетевого экранирования

Для блокировки трафика создается политика межсетевого экранирования с названием *FW-WAN-IN* перечисляются все политики фильтрации, которые были описаны ранее. Для всех правил фильтрации кроме *WEB-server* используется действие *drop*.

Данная последовательность правил реализует цепочку проверок, направленную на очистку паразитного трафика и разрешения установления корректных соединений с сервером.

Поскольку все правила применяются по возрастанию, в политике используется следующая нумерация правил:

- 100-160 – правила с шагом 10 описывают запрещающие правила;
- 500 – разрешает входящий трафик на сервер.

Использование шага 10 в запрещающих правилах позволит, в случае необходимости, добавить дополнительные правила между уже описанными.

Использование номера 500 для разрешающего правила позволяет визуально отделить его от запрещающих правил.

Для всех пакетов, не попавших под цепочку проверок установлено действие drop и включена регистрация в системный журнал.

```
      set policy firewall FW-WAN-IN rule 100 action 'drop'
      set policy firewall FW-WAN-IN rule 100 match filter 'Bogons-
on-WAN'
      set policy firewall FW-WAN-IN rule 110 action 'drop'
      set policy firewall FW-WAN-IN rule 110 match filter 'Bogus-
TCP-Flags'
      set policy firewall FW-WAN-IN rule 120 action 'drop'
      set policy firewall FW-WAN-IN rule 120 match filter 'TCP-
Reset'
      set policy firewall FW-WAN-IN rule 130 action 'drop'
      set policy firewall FW-WAN-IN rule 130 match filter 'Uncommon-
MSS'
      set policy firewall FW-WAN-IN rule 140 action 'drop'
      set policy firewall FW-WAN-IN rule 140 match filter 'New-not-
SYN'
      set policy firewall FW-WAN-IN rule 150 action 'drop'
      set policy firewall FW-WAN-IN rule 150 match filter 'Sync-
flood'
      set policy firewall FW-WAN-IN rule 160 action 'drop'
      set policy firewall FW-WAN-IN rule 160 match filter 'State-
Invalid'
```

```
      set policy firewall FW-WAN-IN rule 500 action 'accept'
      set policy firewall FW-WAN-IN rule 500 match filter 'WEB-
server'
      set policy firewall FW-WAN-IN enable-default-log
      set policy firewall FW-WAN-IN default-action 'drop'
```

5.4. Применение политики МЭ на интерфейс

Созданная политика МЭ применяется для входящего трафика из внешней сети.

```
      set interfaces ethernet eth1 policy in firewall FW-WAN-IN
```